



Cisco CGS 2520 コマンド リファレンス

Cisco IOS Release 12.2(53)EX

2010 年 7 月

【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、すべてユーザー側の責任になります。

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

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

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

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

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。

Cisco CGS 2520 コマンド リファレンス

© 2010 Cisco Systems, Inc. All rights reserved.

Copyright © 2010-2011, シスコシステムズ合同会社.

All rights reserved.



CONTENTS

はじめに	xix
目的	xix
表記法	xix
関連資料	xx
マニュアルの入手方法およびテクニカル サポート	xxi

CHAPTER 1

Command-Line Interface の使用 1-1

CLI コマンド モード	1-1
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	1-3
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	1-4
ライン コンフィギュレーション モード	1-5

CHAPTER 2

Cisco CGS 2520 の Cisco IOS コマンド 2-1

aaa accounting dot1x	2-1
aaa authentication dot1x	2-3
action	2-5
alarm contact	2-7
alarm facility fcs-hysteresis	2-9
alarm facility power-supply	2-10
alarm facility temperature	2-11
alarm profile (グローバル コンフィギュレーション)	2-13
alarm profile (インターフェイス コンフィギュレーション)	2-15
alarm relay-mode	2-17
archive download-sw	2-18
archive tar	2-21
archive upload-sw	2-24
arp access-list	2-26
authentication control-direction	2-28
authentication critical recovery delay	2-30

[authentication event](#) 2-31
[authentication fallback](#) 2-35
[authentication host-mode](#) 2-37
[authentication mac-move permit](#) 2-39
[authentication open](#) 2-41
[authentication order](#) 2-43
[authentication periodic](#) 2-45
[authentication port-control](#) 2-47
[authentication priority](#) 2-49
[authentication timer](#) 2-51
[authentication violation](#) 2-53
[bandwidth](#) 2-55
[boot config-file](#) 2-58
[boot enable-break](#) 2-59
[boot helper](#) 2-60
[boot helper-config-file](#) 2-61
[boot manual](#) 2-62
[boot private-config-file](#) 2-63
[boot system](#) 2-64
[channel-group](#) 2-65
[channel-protocol](#) 2-69
[class](#) 2-71
[class-map](#) 2-73
[clear ip arp inspection log](#) 2-75
[clear ip arp inspection statistics](#) 2-76
[clear ip dhcp snooping](#) 2-77
[clear ipc](#) 2-79
[clear ipv6 dhcp conflict](#) 2-80
[clear l2protocol-tunnel counters](#) 2-81
[clear lacp](#) 2-82
[clear logging onboard](#) 2-83
[clear mac address-table](#) 2-84
[clear mac address-table move update](#) 2-85
[clear pagp](#) 2-86
[clear policer cpu uni-eni counters](#) 2-87

clear port-security	2-88
clear rep counters	2-90
clear scada modbus tcp server statistics	2-91
clear spanning-tree counters	2-92
clear spanning-tree detected-protocols	2-93
clear vmps statistics	2-95
conform-action	2-96
copy logging onboard module	2-98
cpu traffic qos cos	2-100
cpu traffic qos dscp	2-104
cpu traffic qos precedence	2-109
cpu traffic qos qos-group	2-112
define interface-range	2-114
delete	2-116
deny (ARP アクセス リスト コンフィギュレーション)	2-117
deny (IPv6 アクセス リスト コンフィギュレーション)	2-119
deny (MAC アクセス リスト コンフィギュレーション)	2-124
diagnostic monitor	2-127
diagnostic schedule test	2-129
diagnostic start test	2-131
dot1x credentials	2-133
dot1x critical eapol (グローバル コンフィギュレーション)	2-134
dot1x default	2-135
dot1x guest-vlan supplicant	2-136
dot1x initialize	2-137
dot1x max-reauth-req	2-138
dot1x max-req	2-140
dot1x pae	2-141
dot1x supplicant force-multicast	2-143
dot1x system-auth-control	2-144
dot1x test eapol-capable	2-145
dot1x test timeout	2-146
dot1x timeout	2-147
duplex	2-150
errdisable detect cause	2-152

errdisable recovery	2-154
ethernet evc	2-157
ethernet lmi	2-158
ethernet lmi ce-vlan map	2-160
ethernet loopback (イーサネット コンフィギュレーション)	2-162
ethernet loopback (特権 EXEC)	2-165
ethernet oam remote-failure	2-167
ethernet uni	2-169
ethernet uni id	2-171
exceed-action	2-172
fcs-threshold	2-174
flowcontrol	2-175
hw-module module logging onboard	2-177
interface port-channel	2-179
interface range	2-181
interface vlan	2-183
ip access-group	2-185
ip address	2-188
ip arp inspection filter vlan	2-190
ip arp inspection limit	2-192
ip arp inspection log-buffer	2-194
ip arp inspection trust	2-196
ip arp inspection validate	2-197
ip arp inspection vlan	2-199
ip arp inspection vlan logging	2-200
ip device tracking maximum	2-202
ip dhcp snooping	2-203
ip dhcp snooping binding	2-204
ip dhcp snooping database	2-206
ip dhcp snooping information option	2-208
ip dhcp snooping information option allowed-untrusted	2-210
ip dhcp snooping information option format remote-id	2-212
ip dhcp snooping limit rate	2-213
ip dhcp snooping trust	2-214
ip dhcp snooping verify mac-address	2-215

ip dhcp snooping vlan	2-216
ip dhcp snooping vlan information option format-type circuit-id string	2-217
ip igmp filter	2-219
ip igmp max-groups	2-221
ip igmp profile	2-223
ip igmp snooping	2-225
ip igmp snooping last-member-query-interval	2-227
ip igmp snooping querier	2-229
ip igmp snooping report-suppression	2-231
ip igmp snooping tcn	2-233
ip igmp snooping tcn flood	2-235
ip igmp snooping vlan immediate-leave	2-236
ip igmp snooping vlan mrouter	2-237
ip igmp snooping vlan static	2-239
ip sla responder twamp	2-241
ip sla server twamp	2-243
ip source binding	2-245
ip ssh	2-247
ip sticky-arp (グローバル コンフィギュレーション)	2-249
ip sticky-arp (インターフェイス コンフィギュレーション)	2-251
ip verify source	2-253
ipv6 access-list	2-255
ipv6 address dhcp	2-257
ipv6 dhcp client request vendor	2-258
ipv6 dhcp ping packets	2-259
ipv6 dhcp pool	2-261
ipv6 dhcp server	2-264
ipv6 mld snooping	2-266
ipv6 mld snooping last-listener-query-count	2-268
ipv6 mld snooping last-listener-query-interval	2-270
ipv6 mld snooping listener-message-suppression	2-272
ipv6 mld snooping robustness-variable	2-274
ipv6 mld snooping tcn	2-276
ipv6 mld snooping vlan	2-278
ipv6 traffic-filter	2-280

l2protocol-tunnel	2-282
l2protocol-tunnel cos	2-286
lacp port-priority	2-287
lacp system-priority	2-289
link state group	2-291
link state track	2-293
location (グローバル コンフィギュレーション)	2-294
location (インターフェイス コンフィギュレーション)	2-296
logging event	2-298
logging event power-inline-status	2-299
logging file	2-300
mac access-group	2-302
mac access-list extended	2-304
mac address-table aging-time	2-306
mac address-table learning vlan	2-307
mac address-table move update	2-309
mac address-table notification	2-311
mac address-table static	2-313
mac address-table static drop	2-314
macro apply	2-316
macro description	2-318
macro global	2-319
macro global description	2-321
macro name	2-322
match (アクセス マップ コンフィギュレーション)	2-324
match access-group	2-326
match cos	2-327
match ip dscp	2-328
match ip precedence	2-330
match qos-group	2-332
match vlan	2-334
mdix auto	2-337
media-type	2-339
monitor session	2-341
mvr (グローバル コンフィギュレーション)	2-346

mvr (インターフェイス コンフィギュレーション)	2-349
oam protocol cfm svlan	2-352
pagp learn-method	2-353
pagp port-priority	2-355
permit (ARP アクセス リスト コンフィギュレーション)	2-357
permit (IPv6 アクセスリスト コンフィギュレーション)	2-359
permit (MAC アクセス リスト コンフィギュレーション)	2-364
police	2-367
policer aggregate (グローバル コンフィギュレーション)	2-372
police aggregate (ポリシーマップ クラス コンフィギュレーション)	2-377
policer cpu uni	2-379
policy-map	2-381
port-channel load-balance	2-384
port-type	2-386
power inline	2-388
power inline consumption	2-391
power inline police	2-393
priority	2-396
private-vlan	2-399
private-vlan mapping	2-402
queue-limit	2-404
radius-server dead-criteria	2-407
radius-server host	2-409
reload	2-411
remote-span	2-413
renew ip dhcp snooping database	2-415
rep admin vlan	2-417
rep block port	2-418
rep lsl-age-timer	2-421
rep preempt delay	2-423
rep preempt segment	2-425
rep segment	2-426
rep stcn	2-429
reserved-only	2-431
rmon collection stats	2-433

[scada modbus tcp server](#) 2-434
[sdm prefer](#) 2-436
[service instance](#) 2-439
[service password-recovery](#) 2-441
[service-policy \(インターフェイス コンフィギュレーション\)](#) 2-443
[service-policy \(ポリシーマップ クラス コンフィギュレーション\)](#) 2-445
[set cos](#) 2-448
[set dscp](#) 2-450
[set precedence](#) 2-452
[set qos-group](#) 2-454
[setup](#) 2-456
[shape average](#) 2-459
[show access-lists](#) 2-461
[show alarm description port](#) 2-464
[show alarm profile](#) 2-465
[show alarm settings](#) 2-467
[show archive status](#) 2-468
[show arp access-list](#) 2-469
[show authentication](#) 2-470
[show boot](#) 2-474
[show cable-diagnostics tdr](#) 2-476
[show class-map](#) 2-478
[show controllers cpu-interface](#) 2-479
[show controllers ethernet-controller](#) 2-481
[show controllers power inline](#) 2-488
[show controllers tcam](#) 2-490
[show controllers utilization](#) 2-492
[show cpu traffic qos](#) 2-494
[show diagnostic](#) 2-496
[show dot1q-tunnel](#) 2-500
[show dot1x](#) 2-501
[show env](#) 2-504
[show errdisable detect](#) 2-506
[show errdisable flap-values](#) 2-508
[show errdisable recovery](#) 2-510

show etherchannel	2-512
show ethernet loopback	2-515
show ethernet service evc	2-517
show ethernet service instance	2-518
show ethernet service interface	2-520
show facility-alarm relay major	2-522
show facility-alarm status	2-523
show fcs-threshold	2-524
show flowcontrol	2-526
show idprom	2-528
show interfaces	2-531
show interfaces counters	2-540
show interfaces rep	2-542
show interfaces transceivers	2-544
show inventory	2-547
show ip arp inspection	2-548
show ip dhcp snooping	2-552
show ip dhcp snooping binding	2-553
show ip dhcp snooping database	2-555
show ip dhcp snooping statistics	2-557
show ip igmp profile	2-560
show ip igmp snooping	2-561
show ip igmp snooping groups	2-563
show ip igmp snooping mrouter	2-565
show ip igmp snooping querier	2-567
show ip sla standards	2-569
show ip sla twamp connection	2-570
show ip sla twamp session	2-572
show ip source binding	2-574
show ip verify source	2-575
show ipc	2-577
show ipv6 access-list	2-581
show ipv6 dhcp conflict	2-583
show ipv6 route updated	2-584
show l2protocol-tunnel	2-586

[show lacp](#) 2-588
[show link state group](#) 2-592
[show lldp](#) 2-594
[show location](#) 2-595
[show logging onboard](#) 2-598
[show mac access-group](#) 2-602
[show mac address-table](#) 2-604
[show mac address-table address](#) 2-606
[show mac address-table aging-time](#) 2-608
[show mac address-table count](#) 2-610
[show mac address-table dynamic](#) 2-612
[show mac address-table interface](#) 2-614
[show mac address-table learning](#) 2-616
[show mac address-table move update](#) 2-617
[show mac address-table notification](#) 2-619
[show mac address-table static](#) 2-621
[show mac address-table vlan](#) 2-623
[show monitor](#) 2-625
[show mvr](#) 2-628
[show mvr interface](#) 2-630
[show mvr members](#) 2-632
[show pagp](#) 2-634
[show parser macro](#) 2-636
[show policer aggregate](#) 2-638
[show policer cpu uni-eni](#) 2-639
[show policy-map](#) 2-642
[show port-security](#) 2-647
[show port-type](#) 2-650
[show power inline](#) 2-652
[show rep topology](#) 2-657
[show scada modbus tcp server](#) 2-660
[show sdm prefer](#) 2-661
[show spanning-tree](#) 2-663
[show storm-control](#) 2-669
[show system mtu](#) 2-671

show table-map	2-672
show udd	2-674
show version	2-676
show vlan	2-678
show vlan access-map	2-683
show vlan filter	2-684
show vlan mapping	2-685
show vmps	2-687
shutdown	2-689
shutdown vlan	2-690
snmp mib rep trap-rate	2-691
snmp-server enable traps	2-692
snmp-server host	2-697
snmp trap mac-notification change	2-701
spanning-tree	2-703
spanning-tree bpdudfilter	2-705
spanning-tree bpduguard	2-707
spanning-tree cost	2-709
spanning-tree etherchannel guard misconfig	2-711
spanning-tree extend system-id	2-713
spanning-tree guard	2-715
spanning-tree link-type	2-718
spanning-tree loopguard default	2-720
spanning-tree mode	2-722
spanning-tree mst configuration	2-724
spanning-tree mst cost	2-727
spanning-tree mst forward-time	2-729
spanning-tree mst hello-time	2-731
spanning-tree mst max-age	2-733
spanning-tree mst max-hops	2-735
spanning-tree mst port-priority	2-737
spanning-tree mst pre-standard	2-739
spanning-tree mst priority	2-740
spanning-tree mst root	2-742
spanning-tree port-priority	2-744

spanning-tree portfast (グローバル コンフィギュレーション) 2-746

spanning-tree portfast (インターフェイス コンフィギュレーション) 2-749

spanning-tree vlan 2-751

speed 2-754

storm-control 2-756

switchport 2-759

switchport access vlan 2-761

switchport backup interface 2-763

switchport block 2-767

switchport host 2-769

switchport mode 2-770

switchport mode private-vlan 2-773

switchport port-security 2-776

switchport port-security aging 2-780

switchport private-vlan 2-782

switchport protected 2-785

switchport trunk 2-787

switchport vlan mapping 2-789

system env temperature threshold yellow 2-792

system mtu 2-793

table-map 2-795

test cable-diagnostics tdr 2-797

traceroute mac 2-799

traceroute mac ip 2-802

udld 2-804

udld port 2-806

udld reset 2-809

uni count 2-811

uni-vlan 2-813

violate-action 2-815

vlan 2-818

vlan access-map 2-822

vlan dot1q tag native 2-824

vlan filter 2-826

vmmps reconfirm (特権 EXEC) 2-828

vmmps reconfirm (グローバル コンフィギュレーション)	2-829
vmmps retry	2-830
vmmps server	2-831

APPENDIX 3

Cisco CGS 2520 スイッチ Debug コマンド	3-1
debug backup	3-2
debug dot1x	3-3
debug etherchannel	3-4
debug ethernet service	3-5
debug interface	3-7
debug ip dhcp snooping	3-8
debug ip igmp filter	3-9
debug ip igmp max-groups	3-10
debug ip igmp snooping	3-11
debug ip sla error twamp connection	3-12
debug ip sla error twamp control reflector	3-14
debug ip sla error twamp control server	3-16
debug ip sla error twamp session	3-18
debug ip sla trace twamp connection	3-20
debug ip sla trace twamp control reflector	3-22
debug ip sla trace twamp control server	3-24
debug ip sla trace twamp session	3-26
debug ip verify source packet	3-28
debug lacp	3-29
debug mac-notification	3-30
debug matm	3-31
debug matm move update	3-32
debug monitor	3-33
debug mvrdbg	3-34
debug nvram	3-35
debug pagp	3-36
debug platform acl	3-37
debug platform cfm	3-38
debug platform backup interface	3-39
debug platform cpu-queues	3-40
debug platform dot1x	3-42

debug platform etherchannel	3-43
debug platform forw-tcam	3-44
debug platform ip arp inspection	3-45
debug platform ip dhcp	3-46
debug platform ip igmp snooping	3-47
debug platform ip multicast	3-49
debug platform ip source-guard	3-51
debug platform ip unicast	3-52
debug platform ipc	3-54
debug platform led	3-55
debug platform matm	3-56
debug platform messaging application	3-57
debug platform phy	3-58
debug platform pm	3-60
debug platform policer cpu uni-eni	3-62
debug platform port-asic	3-63
debug platform port-security	3-64
debug platform qos-acl-tcam	3-65
debug platform qos-manager	3-66
debug platform remote-commands	3-67
debug platform rep	3-68
debug platform resource-manager	3-69
debug platform snmp	3-70
debug platform span	3-71
debug platform supervisor-asic	3-72
debug platform sw-bridge	3-73
debug platform tcam	3-74
debug platform udid	3-76
debug platform vlan	3-77
debug pm	3-78
debug port-security	3-80
debug qos-manager	3-81
debug scada modbus tcp server	3-82
debug spanning-tree	3-83
debug spanning-tree bpdu	3-85

[debug spanning-tree bpdu-opt](#) 3-86
[debug spanning-tree mstp](#) 3-87
[debug spanning-tree switch](#) 3-89
[debug sw-vlan](#) 3-91
[debug sw-vlan ifs](#) 3-93
[debug sw-vlan notification](#) 3-94
[debug udd](#) 3-96
[debug vqpc](#) 3-98

APPENDIX A**Cisco CGS 2520 スイッチのブート ローダー コマンド A-1**

[boot](#) A-3
[cat](#) A-5
[copy](#) A-6
[delete](#) A-7
[dir](#) A-8
[flash_init](#) A-10
[format](#) A-11
[fsck](#) A-12
[help](#) A-13
[memory](#) A-14
[mkdir](#) A-15
[more](#) A-16
[rename](#) A-17
[reset](#) A-18
[rmdir](#) A-19
[sd_init](#) A-20
[set](#) A-21
[type](#) A-24
[unset](#) A-25
[version](#) A-27

APPENDIX B**Cisco CGS 2520 の Show Platform コマンド B-1**

[show platform acl](#) B-2
[show platform backup interface](#) B-3
[show platform cfm](#) B-4
[show platform configuration](#) B-5

show platform dl B-6

show platform etherchannel B-7

show platform forward B-8

show platform frontend-controller B-10

show platform ip igmp snooping B-11

show platform ip multicast B-13

show platform ip unicast B-14

show platform ipc trace B-16

show platform ipv6 unicast B-17

show platform l2pt dm B-19

show platform layer4op B-20

show platform mac-address-table B-21

show platform messaging B-22

show platform monitor B-23

show platform mvr table B-24

show platform pm B-25

show platform policer cpu B-27

show platform port-asic B-31

show platform port-security B-35

show platform qos B-36

show platform resource-manager B-39

show platform sdflash B-41

show platform snmp counters B-42

show platform spanning-tree synchronization B-43

show platform status B-44

show platform stp-instance B-45

show platform tcam B-46

show platform vlan B-48

show platform vlan mapping B-49

APPENDIX C

オープンソースソフトウェアについて C-1

INDEX



はじめに

目的

Cisco 2520 Connected Grid スイッチ (CGS) (スイッチと呼びます) は、レイヤ 2 の LAN ベース イメージまたはレイヤ 3 の IP Services イメージでサポートされています。

- CGS 2520 の LAN ベース イメージには、Quality of Service (QoS)、柔軟性の高い VLAN 処理、遠隔監視制御・情報取得 (SCADA) プロトコル分類サポート、Resilient Ethernet Protocol (REP) によるリング トポロジでのコンバージェンス時間の改善、Flex Link によるハブ アンド スポーク トポロジにおける高速フェールオーバー、およびセキュリティ機能が含まれています。
- CGS 2520 IP Services イメージでは、IP ルーティング プロトコルのサポート、マルチ VPN ルーティングおよび転送カスタマー エッジ (Multi-VRF CE/VRF-Lite)、ポリシー ベース ルーティング (PBR) などのレイヤ 3 機能が追加されます。

このマニュアルでは、Cisco CGS 2520 スイッチで使用するために作成または変更されたレイヤ 2 およびレイヤ 3 コマンドについて説明します。標準の Cisco IOS Release 12.2 コマンドについては、Cisco.com のホームページで [Service and Support] > [Technical Documents] から Cisco IOS マニュアルセットを参照してください。Cisco Product Documentation のホームページで Cisco IOS Software ドロップダウン リストから [Release 12.2] を選択します。

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。

マニュアルの最新情報については、このリリースのリリース ノートを参照してください。

表記法

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。
- 必ずいずれか 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

Cisco CGS 2520 スイッチ情報サイト：http://www.cisco.com/go/cgs2520_docs



(注)

- 初期設定については、クイック スタート ガイドの「Using Express Setup」の章、またはハードウェア インストール ガイドの付録の「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、Cisco.com にあるリリース ノートの「System Requirements」を参照してください。
- Network Assistant の要件については、Cisco.com の「Getting Started with Cisco Network Assistant」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、次の資料を参照してください。

- 『*Release Notes for the Cisco CGS 2520*』
- 『*Cisco CGS 2520 Software Configuration Guide*』
- 『*Cisco CGS 2520 System Message Guide*』
- 『*Cisco CGS 2520 Hardware Installation Guide*』
- 『*Cisco CGS 2520 Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Cisco CGS 2520*』
- 『*Installation Notes for the Power Supply Modules for the Cisco CGS 2520*』
- 『*Getting Started with Cisco Network Assistant*』
- 『*Release Notes for Cisco Network Assistant*』
- Network Admission Control (NAC) の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- SFP モジュールのインストールに関する注意事項：
http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

- 『Cisco Small Form-Factor Pluggable Modules Installation Notes』
- 『Cisco CWDM GBIC and CWDM SFP Installation Note』
- 互換性マトリクスに関するマニュアル:
http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html
- 『Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix』
- 『Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules』

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

Cisco CGS 2520 スイッチは、Cisco IOS ソフトウェアでサポートされます。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。

コマンドの詳細な説明については、次の項を参照してください。

- これらの機能をサポートするコンフィギュレーション コマンドおよびモニタリング コマンドについては、[第 2 章「Cisco CGS 2520 の 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「Cisco CGS 2520 スイッチのブート 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 3「Cisco CGS 2520 スイッチ Debug 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 B「Cisco CGS 2520 の 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、特に指定がない限り、IP は IP Version 4 (IPv4) を意味します。

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。

以降は、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。
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、端末または不揮発性 RAM (NVRAM) 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、拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を設定したりするには、このモードを使用します。VLAN の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ます。また、**copy running-config startup-config** 特権 EXEC コマンドを使用することにより、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こともできます。VLAN ID 1 ~ 1005 の設定は、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。

VLAN コンフィギュレーション 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)#
```

使用可能な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 の場合、多くの特性を設定することができず、デフォルト設定のままにしておく必要があります。

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** 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

Cisco CGS 2520 の Cisco IOS コマンド

aaa accounting dot1x

認証、認可、およびアカウントिंग（AAA）アカウント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トング方式を、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 アカウント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トング方式を、アカウントング サービス用に使用します。
start-stop	プロセスの開始時に start アカウントング通知を送信し、プロセスの終了時に stop アカウントング通知を送信します。 start アカウントング レコードはバックグラウンドで送信されます。アカウントング サーバが start アカウント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トング レコードをイネーブルにして、アカウントング 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	アカウントング 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。 <ul style="list-style-type: none">• 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 キーワードは、複数入力できます。

■ aaa accounting dot1x

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	変更箇所
12.2(53)EX	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。



(注)

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、**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 accounting dot1x
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)#
```



(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。構文情報については、『Cisco IOS Security Command Reference, Release 12.2』> 「Authentication, Authorization, and Accounting」> 「Authentication Commands」を参照してください。
authentication periodic	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。
authentication timer	再認証の試行の間隔 (秒) を設定します。

aaa authentication dot1x

IEEE 802.1x に準拠するポートで認証、認可、およびアカウントिंग (AAA) 方式を使用するように指定するには **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tring 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	変更箇所
12.2(53)EX	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 サーバとの通信を試みます。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
<code>aaa new-model</code>	AAA アクセス コントロール モデルをイネーブルにします。構文情報については、『 Cisco IOS Security Command Reference, Release 12.2 』> 「 Authentication, Authorization, and Accounting 」> 「 Authentication Commands 」を参照してください。
<code>show running-config</code>	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「 Cisco IOS Commands Master List, Release 12.2 」を選択して、コマンドの項目へ移動します。

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。このアクションをデフォルト値である **forward** に設定するには、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	変更箇所
12.2(53)EX	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。構文情報については、『Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2』> 「IP Services Commands」を選択してください。
ip access-list	名前付きアクセス リストを作成します。構文情報については、『Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2』> 「IP Services Commands」を選択してください。
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 (アクセス 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。

alarm contact

外部アラームのトリガーおよび重大度を設定するには、**alarm contact** 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。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

```
alarm contact {contact-number {description string | severity {critical | major | minor} |
trigger {closed | open}} | all {severity {critical | major | minor} | trigger {closed |
open}}
```

```
no alarm contact {contact-number {description | severity | trigger} | all {severity |
trigger}}
```

<i>contact-number</i>	特定のアラーム接点番号を設定します。指定できる範囲は 1 ~ 4 です。
description string	アラーム接点番号の説明を追加します。説明の文字列の長さは 80 文字以下の英数字にすることができます。この文字列は、アラームのトリガー時に生成されるシステムメッセージに含まれます。
all	すべてのアラーム接点を設定します。
severity	アラームがトリガーされたときに設定される重大度を設定します。重大度はアラーム通知に含まれます。 no alarm contact severity を入力すると、重大度がマイナーに設定されます。
critical	重大度をクリティカルに設定します。
major	重大度をメジャーに設定します。
minor	重大度をマイナーに設定します。
trigger	アラームをトリガーする状態を設定します（接続回線がオープンか、またはクローズか）。 no alarm contact trigger を入力すると、トリガーがクローズに設定されます。
closed	接点がクローズの場合に、アラームがトリガーされることを指定します。
open	接点がオープンの場合に、アラームがトリガーされることを指定します。

デフォルト

アラームは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	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 alarm contact contact-number description は、説明を空の文字列に設定します。

no alarm contact {contact-number | all} severity は、アラーム接点の重大度をマイナーに設定します。

no alarm contact {contact-number | all} trigger は、外部アラーム接点のトリガーをクローズに設定します。

例

次の例は、接点がオープンの際にクリティカルアラームを報告するようにアラーム接点番号 1 を設定する方法を示します。

```
Switch(config)# alarm contact 1 description main_lab_door
Switch(config)# alarm contact 1 severity critical
Switch(config)# alarm contact 1 trigger open
Dec 4 10:34:09.049: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm asserted:
main_lab_door
```

show env alarm-contact または **show running-config** 特権 EXEC コマンドを入力すると、設定を確認できます。

```
Switch# show env alarm-contact
ALARM CONTACT 1
  Status:      asserted
  Description: main_lab_door
  Severity:    critical
  Trigger:     open
```

次の例は、クリア アラーム接点番号 1 と **show** のコマンド出力を設定する方法を示します。

```
Switch(config)# no alarm contact 1 description
Dec 4 10:39:33.621: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared:
main_lab_door Dec 4 10:39:33.621: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm
asserted: external alarm contact 1
```

```
Switch(config)# no alarm contact 1 severity
Dec 4 10:39:46.774: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external
alarm contact 1 Dec 4 10:39:46.774: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm
asserted: external alarm contact 1
```

```
Switch(config)# no alarm contact 1 trigger open
Dec 4 10:39:56.547: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external
alarm contact 1
```

```
Switch(config)# end
Switch# show env alarm-contact
ALARM CONTACT 1
  Status:      not asserted
  Description: external alarm contact 1
  Severity:    minor
  Trigger:     closed
```

```
Switch# show hard led
SWITCH: 1
SYSTEM: GREEN
MGMT: GREEN
ALARM 1: BLACK
ALARM 2: BLACK
ALARM 3: BLACK
ALARM 4: BLACK
```

関連コマンド

コマンド	説明
show env alarm-contact	スイッチのアラーム設定およびステータスを表示します。

alarm facility fcs-hysteresis

フレーム チェック シーケンス (FCS) エラー ヒステリシスしきい値を FCS ビットエラー レートの変動率として設定するには、**alarm facility fcs-hysteresis** 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。FCS エラー ヒステリシスしきい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。

alarm facility fcs-hysteresis percentage

no alarm facility fcs-hysteresis percentage

構文の説明

percentage ヒステリシスしきい値の変動率です。指定できる範囲は 1 ~ 10% です。

デフォルト

デフォルトのしきい値は 10% 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ヒステリシスしきい値を設定すると、設定されたレートの近くまで FCS ビットエラー レートが変動した場合にアラームがトリガーされます。

FCS ヒステリシスしきい値はスイッチすべてのポートで設定します。ポートごとに FCS エラー レートを設定するには、**fcs-threshold** 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。

しきい値がデフォルト値ではない場合、**show running-config** 特権 EXEC コマンドの出力に表示されます。

例

次の例では、FCS エラー ヒステリシスを 5% に設定する方法を示します。ビット エラー レートが設定した FCS ビットエラー レートを 5% 超過するとアラームがトリガーされます。

```
Switch(config)# alarm facility fcs-hysteresis 5
```

関連コマンド

コマンド	説明
fcs-threshold	インターフェイスの FCS エラー レートを設定します。
show running-config	FCS ヒステリシスしきい値 (デフォルト値以外の場合) を含むスイッチの実行コンフィギュレーションを表示します。

alarm facility power-supply

システムがデュアル電源モードで稼動している場合に、電源の欠落または障害を検出するアラーム オプションを設定するには、**alarm facility power-supply** 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。指定した設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

alarm facility power-supply {disable | notifies | relay major | syslog}

no alarm facility power-supply {disable | notifies | relay major | syslog}

構文の説明

disable	電源アラームをディセーブルにします。
notifies	電源装置アラーム トラップを SNMP サーバに送信します。
relay major	リレー回路にアラームを送信します。
Syslog	電源装置アラーム トラップを Syslog サーバに送信します。

デフォルト

電源アラーム メッセージは保存されますが、SNMP サーバ、リレー、または syslog サーバに送信されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

電源アラームは、システムがデュアル電源モードの場合にのみ生成されます。2 つ目の電源が接続された場合、**power-supply dual** 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デュアル電源モードの動作を設定します。

キーワード **notifies** を使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用して SNMP サーバを設定してください。

例

次の例では、電源モニタリング アラームをマイナー リレー回路に送信する設定方法を示します。

```
Switch(config)# alarm facility power-supply relay minor
```

関連コマンド

コマンド	説明
show alarm settings	環境アラーム設定およびオプションが表示されます。
snmp-server enable traps	スイッチでさまざまなトラップの SNMP 通知をネットワーク管理システム (NMS) に送信できるようにします。

alarm facility temperature

プライマリ温度モニタリングアラームの設定または上限値が低いセカンダリ温度アラームしきい値を設定するには、**alarm facility temperature** 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。温度モニタリングアラームの設定を削除またはセカンダリ温度アラームをディセーブルにするには、このコマンドの **no** 形式を使用します。

alarm facility temperature {primary {high | low | notifies | relay major | syslog} | secondary {high | low | notifies | relay major | syslog}}

no alarm facility temperature {primary {high | low | notifies | relay major | syslog} | secondary {high | low | notifies | relay major | syslog}}

構文の説明

high	プライマリ温度アラームまたはセカンダリ温度アラームの高温しきい値を設定します。指定できる範囲は、-238 ~ 572 °F (-150 ~ 300 °C) です。
low	プライマリ温度アラームまたはセカンダリ温度アラームの低温しきい値を設定します。指定できる範囲は、-328 ~ 482 °F (-200 ~ 250 °C) です。
notifies	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを SNMP サーバに送信します。
relay major	プライマリ温度アラームまたはセカンダリ温度アラームがリレー回路に送信されます。
Syslog	プライマリ温度アラーム トラップまたはセカンダリ温度アラーム トラップを Syslog サーバに送信します。

デフォルト

プライマリ温度アラームは -4 ~ 203 °F (-20 ~ 95 °C) の範囲でイネーブルになっており、ディセーブルにできません。アラームはメジャー リレーに関連付けられています。セカンダリ温度アラームはデフォルトで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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

プライマリ温度アラームは自動的にイネーブルになります。アラームはディセーブルにできませんが、アラーム オプションを設定できます。

プライマリ温度アラームの範囲は、**high** および **low** キーワードを使用して設定できます。

温度が最大プライマリ温度のしきい値よりも小さいしきい値に達した場合に高温アラームをトリガーするには、セカンダリ温度アラームを使用します。温度しきい値とアラーム オプションを設定できます。

notifies キーワードを使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用して SNMP サーバを設定してください。

■ alarm facility temperature

例

次の例では、セカンダリ温度の高温しきい値に 113 °F (45 °C) とアラームを設定し、トラップをマイナー リレー回路、syslog、および SNMP サーバに送信する方法を示します。

```
Switch(config)# alarm facility temperature secondary high 45
Switch(config)# alarm facility temperature secondary relay minor
Switch(config)# alarm facility temperature secondary syslog
Switch(config)# alarm facility temperature secondary notifies
```

次の例では、セカンダリ温度アラームをディセーブルにする方法を示します。

```
Switch(config)# no alarm facility temperature secondary 45
```

次の例では、プライマリ温度アラームを設定し、syslog とメジャー リレー回路にアラームとトラップを送信する方法を示します。

```
Switch(config)# alarm facility temperature primary syslog
Switch(config)# alarm facility temperature primary relay major
```

関連コマンド

コマンド	説明
show alarm settings	環境アラーム設定およびオプションが表示されます。
snmp-server enable traps	スイッチでさまざまなトラップ タイプ SNMP 通知を Network Management System (NMS; ネットワーク管理システム) に送信します。

alarm profile (グローバル コンフィギュレーション)

アラーム プロファイルを作成し、アラーム 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、**alarm 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。アラーム 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。

alarm profile name

no alarm profile name

構文の説明

<i>name</i>	アラームのプロファイル名です。
-------------	-----------------

デフォルト

アラーム プロファイルは作成されません。
プロファイルを作成しても、アラームは1つもイネーブルになりません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

アラームプロファイル モードの使用可能なコマンド：

- **alarm alarm-id** : 特定のアラームがイネーブルになります。
- **exit** : アラームプロファイル コンフィギュレーション モードを終了します。
- **help** : インタラクティブ ヘルプ システムの説明が表示されます。
- **no** : コマンドを無効にするか、デフォルトに設定します。
- **notifies alarm-id** : アラームの通知がイネーブルになり、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) トラップが SNMP サーバに送信されます。
- **relay-major alarm-id** : アラームがメジャー リレー回路に送信されます。
- **relay-minor alarm-id** : アラームがマイナー リレー回路に送信されます。
- **syslog alarm-id** : アラームが syslog ファイルに送信されます。

alarm-id には、アラーム ID を 1 つまたはスペースで区切って複数入力します。

キーワード **notifies** を使用してアラーム トラップを SNMP ホストに送信する前に、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用して SNMP サーバを設定してください。

インターフェイスにはすべて、デフォルトプロファイルが存在します。**show alarm profile** ユーザ EXEC コマンドを入力して **defaultPort** の出力を確認してください。

表 2-1 AlarmList ID 番号とアラームの説明

AlarmList ID	アラームの説明
1	リンク障害です。
2	ポートでフォワーディングされません。
3	ポートが動作していません。
4	FCS エラー レートがしきい値を超過しています。

アラーム プロファイルを作成すると、**alarm-profile** 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、プロファイルをインターフェイスに関連付けられます。

デフォルトでは、**defaultPort** プロファイルはすべてのインターフェイスに適用されます。このプロファイルによって、ポートが動作していない (3) アラームのみがイネーブルになります。このプロファイルは、**alarm profile defaultPort** グローバル コンフィギュレーション コマンドを使用し、アラーム プロファイル コンフィギュレーション モードを開始して変更できます。

例

次の例では、ポートのリンク障害 (アラーム 1) とポートでフォワーディングされない (アラーム 2) アラームがイネーブルのアラーム プロファイル **fastE** を作成する方法を示します。リンク障害アラームはマイナー リレー回路に関連付けられており、ポートでフォワーディングされないアラームはメジャーリレー回路に関連付けられています。このアラームは SNMP サーバに送信され、システム ログ ファイル (syslog) に書き込まれます。

```
Switch(config)# alarm profile fastE
Switch(config-alarm-prof)# alarm 1 2
Switch(config-alarm-prof)# relay major 2
Switch(config-alarm-prof)# relay minor 1
Switch(config-alarm-prof)# notifies 1 2
Switch(config-alarm-prof)# syslog 1 2
```

次の例では、**my-profile** という名前のアラーム リレー プロファイルを削除する方法を示します。

```
Switch(config)# no alarm profile my-profile
```

関連コマンド

コマンド	説明
alarm profile (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アラーム プロファイルに関連付けます。
show alarm settings	アラーム プロファイルすべてまたは指定したアラーム プロファイルを表示し、それぞれのプロファイルが関連付けられているインターフェイスをリスト表示します。
snmp-server enable traps	スイッチでさまざまなトラップ タイプ SNMP 通知を Network Management System (NMS; ネットワーク管理システム) に送信します。

alarm profile (インターフェイス コンフィギュレーション)

アラーム プロファイルをポートに関連付けるには、**alarm profile** 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。ポートからプロファイルの関連付けを解除するには、このコマンドの **no** 形式を使用します。

alarm profile *name*

no alarm profile

構文の説明

<i>name</i>	アラームのプロファイル名です。
-------------	-----------------

デフォルト

アラーム プロファイル *defaultPort* がすべてのインターフェイスに適用されています。このプロファイルでは、ポートが動作していないアラームのみがイネーブルです。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

アラーム プロファイルを作成して、アラームを 1 つ以上イネーブルにし、アラーム オプションを指定するには、**alarm 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。

インターフェイスに関連付けられるアラーム プロファイルは 1 つのみです。

アラーム プロファイルをインターフェイスに関連付けると、そのインターフェイスにすでに関連付けられていたアラーム プロファイルは上書きされます (*defaultPort* プロファイルを含む)。

例

次の例では、ポートにアラーム プロファイル *fastE* を関連付ける方法を示します。

```
Switch(config)# interface fastethernet1/2
Switch(config-if)# alarm profile fastE
```

次の例では、ポートからアラーム プロファイルの関連付けを解除して、*defaultPort* プロファイルに戻す方法を示します。

```
Switch(config)# interface fastethernet1/2
Switch(config-if)# no alarm profile
```

■ alarm profile (インターフェイス コンフィギュレーション)

関連コマンド.	コマンド	説明
	alarm profile (グローバル コンフィギュレーション)	アラーム プロファイルを作成および指定して、アラームプロファイル コンフィギュレーション モードが開始されます。
	show alarm settings	アラーム プロファイルすべてまたは指定したアラーム プロファイルを 表示し、それぞれのプロファイルが関連付けられているインターフェ イスをリスト表示します。

alarm relay-mode

スイッチのアラーム リレー モードをポジティブまたはネガティブに設定するには、**alarm relay-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。アラーム リレー モードをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

alarm relay-mode {*negative*}

no alarm relay-mode {*negative*}

構文の説明

negative アラーム リレー モードをネガティブに設定します。

デフォルト

デフォルトでは、アラーム リレーがオープンされると、ポジティブ モードに設定されます。スイッチの電源がオフの場合、アラーム リレーはすべてオープンです。アラーム イベントが 1 つ以上検出されると、アラーム リレーはクローズされます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

アラーム リレーの動作を元に戻すには、このコマンドを使用します。アラーム リレー モードがネガティブに設定されている場合、アラーム リレーは通常クローズされています。アラーム イベントが 1 つ以上検出されると、該当するアラーム リレーがオープンされます。

例

次の例では、アラーム リレーをネガティブ モードに設定する方法を示します。

```
Switch(config)# alarm relay-mode negative
```

関連コマンド

コマンド	説明
alarm profile (グローバル コンフィギュレーション)	アラーム プロファイルを作成および指定して、アラームプロファイル コンフィギュレーション モードが開始されます。
show alarm profile	アラーム プロファイルすべてまたは指定したアラーム プロファイルを表示し、それぞれのプロファイルが関連付けられているインターフェイスをリスト表示します。
show alarm settings	環境アラーム設定およびオプションが表示されます。

archive download-sw

新しいイメージを TFTP サーバから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持するには、**archive download-sw** 特権 EXEC コマンドを使用します。

```
archive download-sw {/force-reload | /imageonly | /leave-old-sw | /no-set-boot |
/no-version-check | /overwrite | /reload | /safe | /warm} source-url
```

構文の説明

/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	互換性のないイメージをインストールしないように確認せずに、ソフトウェア イメージをダウンロードします。
/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。

<code>/warm</code>	イメージをダウンロードしたら、ストレージからイメージを読み取らずにスイッチをリロードします。
<code>source-url</code>	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。 <ul style="list-style-type: none"> 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]/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： rpc:[[/username@location]/directory]/image-name.tar TFTP の構文： tftp:[[/location]/directory]/image-name.tar <p><i>image-name.tar</i> 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。</p>

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せん。ダウンロードするイメージでのバージョンの互換性がチェックされます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

`/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く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、エラーが発生しません。

/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.2-116) を参照してください。



(注)

/no-version-check オプションの使用には注意が必要です。このオプションを使用すると、最初にイメージにスイッチとの互換性があることを確認せずにイメージをダウンロードできます。

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。

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
```

関連コマンド

コマンド	説明
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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 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 Remote Copy Protocol (RCP) の構文： rcp:[[/username@location]/directory]/tar-filename.tar TFTP の構文：tftp:[[/location]/directory]/tar-filename.tar <p>tar-filename.tar は、作成する tar ファイルです。</p> <p>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。</p> <p>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。</p>
/table source-url	<p>既存の tar ファイルの内容を画面に表示します。</p> <p>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。</p> <ul style="list-style-type: none"> 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 RCP の構文： rcp:[[/username@location]/directory]/tar-filename.tar TFTP の構文：tftp:[[/location]/directory]/tar-filename.tar <p>tar-filename.tar は、表示する tar ファイルです。</p>

<pre>/xtract source-url flash:/file-url [dir/file...]</pre>	<p>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。</p> <p><i>source-url</i> 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。</p> <ul style="list-style-type: none"> 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 RCP の構文 : rpc:[/username@location]/directory]/tar-filename.tar TFTP の構文 : tftp:[[/location]/directory]/tar-filename.tar <p><i>tar-filename.tar</i> は、抽出される tar ファイルです。</p> <p>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、<i>dir/file...</i> 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。</p>
---	--

デフォルト なし

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更箇所
	12.2(53)EX	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:image_name-mz.122-release.tar
info (219 bytes)
image_name-mz.122-release/(directory)
image_name-mz.122-release(610856 bytes)
image_name-mz.122-release/info (219 bytes)
info.ver (219 bytes)
```

次の例は、*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。

```
Switch# archive tar /table flash:image_name-mz.122-release.tar
image_name-mz.122-release/html
image_name-mz.122-release/html/ (directory)
image_name-mz.122-release/html/const.htm (556 bytes)
image_name-mz.122-release/html/xhome.htm (9373 bytes)
image_name-mz.122-release/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 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 [/version *version_string*] **destination-url**

構文の説明

/version <i>version_string</i>	(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。 <ul style="list-style-type: none"> 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]/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 <i>image-name.tar</i> 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

flash: 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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、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 tftp://172.20.140.2/test-image.tar
```

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

<i>acl-name</i>	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	変更箇所
12.2(53)EX	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.2-117) 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.2-357) 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 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 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	変更箇所
12.2(53)EX	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タス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 critical recovery delay

Auth Manager のクリティカルな回復遅延を設定するには、グローバル コンフィギュレーション モードで **authentication critical recovery delay** コマンドを使用します。以前に設定した回復遅延を削除するには、このコマンドの **no** 形式を使用します。

authentication critical recovery delay *milliseconds*

no authentication critical recovery delay

構文の説明

<i>milliseconds</i>	使用不可になっていた RADIUS サーバが使用可能になったときに、クリティカル ポートの再初期化を Auth Manager が待機する時間（ミリ秒単位）です。有効な値は 1 ～ 10000 です。
---------------------	--

コマンド デフォルト

デフォルト遅延は 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例は、クリティカルな回復遅延時間を 1500 ミリ秒に設定する方法を示します。

```
Switch(config)# authentication critical recovery delay 1500
```

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、アカウントリング) 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。

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	変更箇所
12.2(53)EX	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 **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 IEEE 802.1x 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 :

- サブ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ブリカントに送信されます。これは、サブ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、サブリカントは 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 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、サブリカントの 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タスのままになります。

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。

```
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。ポートをマルチホスト モードまたはマルチ認証モードにするには、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。

コマンド	説明
authentication port-control	ポートの認証ステータス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	変更箇所
12.2(53)EX	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タス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

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

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

no authentication host-mode [multi-auth | 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-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	変更箇所
12.2(53)EX	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。

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 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タス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	変更箇所
12.2(53)EX	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またはディセーブにします。
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	変更箇所
12.2(53)EX	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タス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 Authentication Bypass (MAB; MAC 認証バイパス) 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	変更箇所
12.2(53)EX	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 番めの方式として MAB を、3 番めの方式として 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 番めの認証方式として 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タス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	変更箇所
	12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン 定期的に再認証を行う間隔の時間を設定するには、**authentication timer reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。

例 次の例では、ポートの定期的再認証をイネーブ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タスの手動制御をイネーブにします。
	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 許可ステータス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、許可ステータスまたは無許可ステータスに変わります。
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、許可ステータスに変わります。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、無許可ステータスに変わります。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	変更箇所
12.2(53)EX	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、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、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、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、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、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; スイッチド ポート アナライザ) 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 ステートを自動的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 ステータス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 ステータス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 Authentication Bypass (MAB; MAC 認証バイパス) 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	変更箇所
12.2(53)EX	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タス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]} {restart value}
```

```
no authentication timer {[inactivity | reauthenticate]} {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。
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** および **restart** は、オフに設定されています。**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	変更箇所
12.2(53)EX	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タス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 | restrict | shutdown | replace}

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

構文の説明

protect	予期しない着信 MAC アドレスがドロップされます。syslog エラーは生成されません。
restrict	違反エラーが発生し、着信 MAC アドレスがドロップされると、Syslog エラーが生成されます。
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。
replace	古いセッションを切断し、着信 MAC アドレスを使用して認証シーケンスを開始します。

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	変更箇所
12.2(53)EX	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された場合にシステム エラー メッセージを生成し、制限モードに切り替わるように 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 restrict
```

次の例では、新しいデバイスがポートに接続された場合にその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)# authentication violation protect
```

次の例は、新しいデバイスがポートに接続された場合に、古いセッションを切断して、新しいデバイスを認証する単一ホスト モードである 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 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	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タス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。

bandwidth

ポリシーマップ クラスの出力帯域幅を設定して、クラスベース均等化キューイング (CBWFQ) を設定するには、**bandwidth** 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。クラスの帯域幅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。

bandwidth {*rate* | *percent value* | *remaining percent value*}

no bandwidth [*rate* | *percent value* | *remaining percent value*]

構文の説明

<i>rate</i>	クラスの帯域幅レートをキロビット/秒 (kb/s) 単位で設定します。指定できる範囲は 64 ~ 1000000 です。
<i>percent value</i>	合計帯域幅の割合としてクラスの帯域幅を設定します。指定できる範囲は 1 ~ 100% です。
<i>remaining percent value</i>	残りの帯域幅の割合としてクラスの帯域幅を設定します。指定できる範囲は 1 ~ 100% です。

デフォルト

帯域幅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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

出力トラフィックを制御するには、**bandwidth** ポリシーマップ クラス コマンドを使用します。**bandwidth** コマンドは、そのクラス内のトラフィックの帯域幅を指定します。CBWFQ はクラスに割り当てられた帯域幅から、クラスに属するパケットの重み付けを取得し、この重み付けを使用して、このクラスのキューが適正に処理されるようにします。帯域幅設定は、入力ポリシー マップでサポートされません。

トラフィックのクラスの帯域幅を絶対レート (kb/s) または帯域幅に対する割合 (**percent value**) として設定すると、その帯域幅はそのトラフィック クラスの最小帯域幅保証または認定情報レート (CIR) を表します。つまり、トラフィック クラスは最低でもコマンドにより指定された帯域幅を取得しますが、その帯域幅に制限されるわけではありません。ポートの超過帯域幅はすべて、設定済み CIR レートと同じ比率で各クラスに割り当てられます。

bandwidth remaining percent コマンドを入力すると、絶対帯域幅が保証されず、相対帯域幅のみが確認されます。クラスの帯域幅は、常に、ポートに設定された指定帯域幅の割合に比例します。

出力ポリシーで帯域幅を設定する場合、各帯域幅設定で同じ単位を指定する必要があります。つまり、すべての絶対値 (レート) にするか、またはパーセントにします。

ポリシーの各キューにおける最小帯域幅保証の合計速度は、インターフェイスの合計速度を上回ることはできません。**percent** キーワードが使用されている場合、クラスの帯域幅の割合の合計が 100% を超えることはできません。

queue-limit コマンドを使用してデフォルトのキュー制限を変更すると、インターフェイスに必要な最小帯域幅保証を満たすことができるため、高速のインターフェイスで特に重要です。

bandwidth 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 CBWFQ を設定したり、**shape average** コマンドを使用してポリシー マップの同じクラスのクラスベース シェーピングを設定したりすることはできません。

プライオリティ キューイング (**priority** 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設定) を含むクラスの帯域幅は設定できません。

例

次に、帯域幅 (kbps) を設定することにより、出力キューの優先順位を設定する例を示します。クラス *outclass1*、*outclass2*、および *outclass3* は、それぞれ 50000、20000、および 10000 kb/s の最小帯域幅を取得します。クラス **class-default** は、最低限として、残りの帯域幅を取得します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 50000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

次に、各トラフィック クラスに、使用可能な合計帯域幅の割合を割り当てることで、出力キューの優先順位を設定する例を示します。クラス *outclass1*、*outclass2* および *outclass3* は、それぞれ 50、20、および 10% の最小帯域幅を取得します。クラス **class-default** は、最低限 20% の帯域幅を取得します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

次に、プライオリティ キューとして *outclass1* を設定し、プライオリティ キューが処理された後に *outclass2* および *outclass3* がそれぞれ残りの帯域幅の 50% および 20% を取得するように設定する例を示します。クラス **class-default** は、保証なしで、残りの 30% を取得します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# 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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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	Quality of Service (QoS) ポリシー マップを表示します。

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するには、**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	変更箇所
12.2(53)EX	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。

このコマンドは、CONFIG_FILE 環境変数の設定を変更します。詳細については、[付録 A 「Cisco CGS 2520 スイッチのブート 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、**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** 形式を使用しません。

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。コンソール上でブレイク 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	変更箇所
12.2(53)EX	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と、フラッシュ ファイル システムが初期化された後にブレイク キーを押して、自動ブートプロセスを中断できます。ブレイク キーは、オペレーティング システムごとに異なります。

- UNIX を実行している SUN ワークステーションでは、Ctrl+C がブレイク キーです。
- Windows 2000 を実行する PC では、Ctrl+Break がブレイク キーとなります。

このコマンドは、ENABLE_BREAK 環境変数の設定を変更します。詳細については、付録 A 「Cisco CGS 2520 スイッチのブート 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

<i>filesystem:</i>	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。
<i>/file-url</i>	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	変更箇所
12.2(53)EX	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。詳細については、[付録 A 「Cisco CGS 2520 スイッチのブート 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		
<i>filesystem:</i>		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。
<i>/file-url</i>		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	変更箇所
	12.2(53)EX	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。詳細については、[付録 A 「Cisco CGS 2520 スイッチのブート 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

次のブート 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、**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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

システムを次回リブートすると、スイッチはブート ロードер 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 ロード 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。詳細については、[付録 A 「Cisco CGS 2520 スイッチのブート ロード 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

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するには、**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

<i>filename</i>	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	変更箇所
12.2(53)EX	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 ...*

no boot system

構文の説明

<i>filesystem:</i>	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。
<i>/file-url</i>	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。

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ブートしようとします。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	変更箇所
12.2(53)EX	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。

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。詳細については、[付録 A 「Cisco CGS 2520 スイッチのブート 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。

channel-group

EtherChannel グループにイーサネット ポートを割り当てるには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用します。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
```



(注)

Link Aggregation Control Protocol (LACP) およびポート集約プロトコル (PAgP) は、ネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でだけ使用できます。**active**、**auto**、**desirable**、および **passive** キーワードは、ユーザ ネットワーク インターフェイス (UNI) では表示されません。

構文の説明

<i>channel-group-number</i>	チャンネル 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 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。チャンネルは、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	PAgP デバイス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。チャンネルは、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。相手側のポート グループが desirable または auto モードの場合にチャンネルが形成されます。 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。

channel-group

on	<p>on モードをイネーブルにします。</p> <p>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。</p>
passive	<p>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。</p> <p>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。チャンネルは、active モードの別のポートグループでだけ形成されます。</p>

デフォルト

チャン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	変更箇所
12.2(53)EX	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 EtherChannel の場合、物理ポートをチャン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ン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、チャン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ンネルインターフェイスが作成されます。最初にポートチャン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ンネルを作成します。

ポートが UNI または ENI の場合、**channel-group** コマンドを使用する前に、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。NNI はデフォルトでイネーブルです。

チャン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 のポートチャンネルを作成できます。インターフェイスをチャンネルグループに適用する前に、ポートチャン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、ポートチャンネルインターフェイスに加えられた設定の変更は、そのポートチャン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、ポートチャン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、チャン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**

モードを **on** に設定（手動設定）する場合は、慎重に実行する必要があります。**on** モードに設定したすべてのポートは、同じグループにバンドルされており、同様の特性を持つようになります。グループの設定を誤ると、パケット損失またはスパンニングツリーループが発生することがあります。

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 が稼動している複数の EtherChannel グループは、同じスイッチ上で共存できます。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。

**(注)**

PAgP および LACP は、NNI および ENI 上でだけ使用できます。

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 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。

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

次に、EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセスポート 2 つを PAgP モード **desirable** であるチャンネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -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
```

次に、EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセスポート 2 つを LACP モード **active** であるチャンネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -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
```

channel-group

```
Switch(config-if-range)# 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
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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

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; ポート集約プロトコル) 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	変更箇所
12.2(53)EX	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。



(注)

PAgP および LACP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

ポートがユーザ ネットワーク インターフェイス (UNI) または ENI の場合、**channel-protocol** コマンドを使用する前に、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。NNI はデフォルトでイネーブルです。

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。

■ channel-protocol

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。

class

ポリシーを作成、変更、またはポリシーを設定する前にポリシーにシステムのデフォルト クラスを指定するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始するには、**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。ポリシー マップからクラスを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

<i>class-map-name</i>	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作成されたクラス マップの名前。
class-default	システムのデフォルト クラス。このクラスは、すべての分類されないトラフィックと一致します。デフォルト クラスは作成または削除できません。

デフォルト

ポリシー マップ クラス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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポリシーマップ コンフィギュレーション モードで **class class-map-name** コマンドを使用する前に、**class-map class-map-name** グローバル コンフィギュレーション コマンドを使用して、クラスを作成する必要があります。**class-default** クラスは、トラフィックが設定されているクラス マップのいずれの一致基準とも一致しない場合に、そのトラフィックが送られるクラスです。

ポリシー マップを指定し、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。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。

入力ポリシー マップの最大クラス数は 64 + **class-default** です。

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。

- **bandwidth** : ポリシー マップに属しているクラスに割り当てる帯域幅を指定します。詳細については、**bandwidth** コマンドを参照してください。
- **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にそれぞれ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 コンフィギュレーション)** ポリシーマップ クラス コマンドを参照してください。
- **priority** : このクラスに厳密なスケジューリング プライオリティを設定します。または、**police** キーワードと併用して、ポリシングを含むプライオリティを設定します。詳細については、**priority** ポリシーマップ クラス コマンドを参照してください。
- **queue-limit** : 重み付きテールドロップ (WTD) のキューの最大しきい値を設定します。詳細については、**queue-limit** コマンドを参照してください。
- **service-policy** : QoS サービス ポリシーを設定して、入力ポリシーまたは出力ポリシーの親ポリシー マップに適用します。詳細については、**service-policy (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。詳細については、**set** コマンドを参照してください。
- **shape average** : 平均トラフィック シェーピング レートを指定します。詳細については、**shape average** 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。

例

次に、ポリシー マップ *policy1* を作成し、クラス *class1* を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始してクラスの基準を設定する例を示します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
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-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。
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 policy-map interface [interface-id]	(任意) 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に設定されているポリシー マップを表示します。

class-map

指定した基準とパケットのマッチングに使用されるクラス 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 マップを削除する場合は、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。パケットがすべての一致基準を満たす必要があります。
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。パケットが1つまたは複数の一致基準を満たす必要があります。
<i>class-map-name</i>	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** のいずれのキーワードも指定しない場合、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	変更箇所
12.2(53)EX	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。

スイッチでは、最大 1024 の一意のクラス マップをサポートしています。

ポート単位で適用されるグローバルに名付けられたサービス ポリシーの一部としてパケット分類を定義するには、**class-map** コマンドとクラスマップ コンフィギュレーション モードを使用します。クラス マップを設定したら、1つまたは複数の **match** コマンドを使用して一致基準を指定できます。入力インターフェイスまたは出力インターフェイスのいずれかに到達 (**service-policy** インターフェイス コンフィギュレーション コマンドの設定によって決定されます) するパケットは、クラスマップの一致基準に照らしてチェックされ、パケットがそのクラスに属しているかどうか判断されます。

match-all クラス マップは、パケットがすべてのエントリと一致する必要があり、他の一致ステートメントがない可能性があることを意味します。

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

- **description** : クラス マップを説明します (最大 200 文字)。**show class-map** 特権 EXEC コマンドを実行すると、クラス マップの説明と名前が表示されます。
- **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。詳細については、**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。

例

次の例は、*class1* というクラス マップの設定方法を示します。デフォルトでは、クラス マップは **match-all** であるため、他の一致基準が含まれない場合があります。

```
Switch(config)# class-map class1
Switch(config-cmap)# exit
```

次の例は、一致基準が 1 つの **match-any** クラス マップ (アクセス リスト *103*) を設定する方法を示します。このクラス マップ (ACL に一致) は、入力ポリシー マップでだけサポートされます。

```
Switch(config)# class-map class2
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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
match access-group	指定したアクセス コントロール リスト (ACL) に基づいて、クラス マップの一致基準を設定します
match cos	レイヤ 2 サービス クラス (CoS) マーキングに基づいて、クラス マップの一致基準を設定します。
match ip dscp	特定の IPv4 の DiffServ コード ポイント (DSCP) 値に基づいて、クラス マップの一致基準を設定します。
match ip precedence	IPv4 precedence 値に基づいて、クラス マップの一致基準を設定します。
match qos-group	特定の Quality of Service (QoS) グループ値に基づいて、クラス マップの一致基準を設定します。
match vlan	VLAN ID または一連の VLAN ID に基づいて、階層型ポリシー マップの親ポリシーのクラス マップの一致基準を設定します。
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 ip arp inspection log

ダイナミック アドレス解決プロトコル (ARP) インスペクション ログ バッファを消去するには、**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	変更箇所
12.2(53)EX	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 Access Control List (ACL; アクセス コントロール リスト) 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 ip arp inspection 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	変更箇所
12.2(53)EX	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 ip arp inspection 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 バインディング データベース エージェント統計情報または DHCP スヌーピング統計情報カウンタを消去するには、**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。
<i>ip-address</i>	バインディング エントリ IP アドレスをクリアします。
interface <i>interface-id</i>	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 <i>vlan-id</i>	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。
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	変更箇所
12.2(53)EX	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 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。

```
Switch# clear ip dhcp snooping database 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 database** 特権 EXEC コマンドを入力します。

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。

■ clear ip dhcp snooping

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	statistics
	IPC キューの統計情報をクリアします。	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	変更箇所
	12.2(53)EX	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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

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	変更箇所
12.2(53)EX	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 | routing | 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。クライアントはネイバー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られません。

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消去するには、**clear l2protocol-tunnel counters** 特権 EXEC コマンドを使用します。

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

このコマンドは、スイッチでメトロ IP アクセス イメージまたはメトロ アクセス イメージが稼動している場合にのみサポートされます。

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	変更箇所
12.2(53)EX	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 gigabitethernet0/2
```

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) チャンネル 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}
```



(注)

LACP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

構文の説明

<i>channel-group-number</i>	(任意) チャンネル 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	変更箇所
12.2(53)EX	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 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、指定のチャンネル 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、すべてのチャンネル 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 チャンネル グループ情報を表示します。

clear logging onboard

フラッシュ メモリに保存されている稼働時間と CLI コマンド情報以外のすべてのオンボード障害ロギング (OBFL) を消去するには、**clear logging onboard** 特権 EXEC コマンドを使用します。

clear logging onboard [module {slot-number | all}]

構文の説明	module (任意) スロット番号は常に 1 で、CGS 2520 には関連しません。 clear logging {slot-number all} onboard module 1 または clear logging onboard all を入力した結果は、 clear logging onboard を入力した結果と同じになります。
--------------	--

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 変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン OBFL はイネーブルにしておき、フラッシュ メモリに保存されたデータは消さないようにすることを推奨します。

例 次の例に、稼働時間と CLI コマンド情報以外のすべての OBFL 情報を消去する方法を示します。

```
Switch# clear logging onboard
Clear logging onboard buffer [confirm]
PID: CGS-2520-24TC , VID: 03 , SN: FOC1225U4CY
```

```
Switch# clear logging onboard module all
Clear logging onboard buffer [confirm]
PID: CGS-2520-24TC , VID: 03 , SN: FOC1225U4CY
```

情報が消去されたかどうかを確認するには、**show logging onboard onboard** 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
	hw-module module logging onboard OBFL をイネーブルにします。
	show logging onboard OBFL 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、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 <i>mac-addr</i>	(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 <i>interface-id</i>	(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 <i>vlan-id</i>	(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 ~ 4096 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

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 address-table	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

このコマンドは、スイッチでメトロ IP アクセス イメージまたはメトロ アクセス イメージが稼動している場合にのみサポートされます。

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。

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	変更箇所
12.2(53)EX	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	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 pagp

Port Aggregation Protocol (PAgP; ポート集約プロトコル) チャンネル 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}
```



(注)

PAgP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

構文の説明

<i>channel-group-number</i>	(任意) チャンネル 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

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、指定のチャンネル 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、すべてのチャンネル 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 チャンネル グループ情報を表示します。

clear policer cpu uni-eni counters

コントロールプレーンポリサー統計情報を消去するには、**clear policer cpu uni-eni counters** 特権 EXEC コマンドを使用します。コントロールプレーンポリサーは、ユーザネットワークインターフェイス (UNI) および拡張ネットワークインターフェイス (ENI) から制御パケットをドロップまたはレート制限して、CPU を過負荷から保護します。

clear policer cpu uni-eni counters {classification | drop}

構文の説明

classification	機能によって統計情報を維持するコントロールプレーンポリサー分類カウンタを消去します。
drop	コントロールプレーンポリサーで維持されるすべてのフレームドロップ統計情報を消去します。

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

ユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	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、機能またはドロップされたフレームに関する統計情報ごとに維持される統計情報を消去できます。

clear コマンドを使用する前後に機能の統計情報またはドロップされたフレームを表示するには、**show platform policer cpu classification** コマンドまたは **show policer cpu uni drop** コマンドを入力します。

関連コマンド

コマンド	説明
show platform policer cpu classification	機能ごとの CPU ポリサー統計情報を表示します。
show policer cpu uni-eni	スイッチの CPU ポリサー情報を表示します。

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、またはスティッキー）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。 <ul style="list-style-type: none"> 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。

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	変更箇所
12.2(53)EX	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 gigabitethernet0/1
```

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 rep counters

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 Resilient Ethernet Protocol (REP; レジリエントイーサネットプロトコル) カウンタをクリアするには、**clear rep counters** 特権 EXEC コマンドを使用します。

clear rep counters [*interface interface-id*]

構文の説明

interface interface-id (任意) カウンタをクリアする REP インターフェイスを指定します。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

すべての REP カウンタをクリアするには、**clear rep counters** コマンドを使用します。また、**clear rep counters interface interface-id** コマンドを使用すると、そのインターフェイスのカウンタだけをクリアできます。

clear rep counters コマンドを入力すると、**show interface rep detail** コマンドの出力に表示されるカウンタだけをクリアできます。SNMP に表示されるカウンタは読み取り専用であるため、クリアできません。

例

次の例では、すべての REP インターフェイスのすべての REP カウンタをクリアする方法を示します。

```
Switch# clear rep counters
```

REP 情報が削除されたかどうかを確認するには、**show interfaces rep 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
show interfaces rep detail	REP の設定およびステータス情報の詳細を表示します。

clear scada modbus tcp server statistics

MODBUS TCP サーバおよびクライアントの統計情報を消去するには、**clear scada modbus tcp server statistics** 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。

clear scada modbus tcp server 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

```
Switch# clear scada modbus tcp server statistics
```

統計情報が消去されたかどうかを確認するには、**show scada modbus tcp server [connections]** 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
scada modbus tcp server	スイッチ上で MODBUS TCP をイネーブルにします。スイッチは、MODBUS TCP サーバとして機能します。
show scada modbus tcp server [connections]	サーバ情報および統計情報を表示します。クライアント情報および統計情報を表示するには、 connection キーワードを使用します。

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は、物理ネットワーク ノード インターフェイス (NNI)、スパニング ツリーがイネーブルになっている拡張 ネットワーク インターフェイス (ENI)、VLAN、スパニング ツリー ポート チャンネルなどです。指定できる VLAN 範囲は 1 ~ 4094 です。ポート チャンネル範囲は 1 ~ 48 です。

(注) スパニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。このコマンドは、コマンドラインのヘルプには表示されますが、STP を実行していない UNI または ENI では無効です。

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	変更箇所
12.2(53)EX	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 STP ポートのスパニング ツリー カウンタが消去されます。

例

次の例は、すべての STP ポートのスパニング ツリー カウンタを消去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

すべてのスパンニング ツリー 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（ネイバー 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は、物理ネットワーク ノード インターフェイス (NNI)、スパンニング ツリーがイネーブルになっている拡張ネットワーク インターフェイス (ENI)、VLAN、ポート チャネルなどです。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。
(注)	スパンニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。このコマンドは、コマンドラインのヘルプには表示されますが、STP を実行していない UNI または ENI では無効です。

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	変更箇所
12.2(53)EX	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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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; 高速スパンニング 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、それ以上 IEEE 802.1D BPDU を受信しなければ、スイッチが自動的に Rapid-PVST+ または MSTP モードに戻ることはありません。レガシー スイッチが指定スイッチでない限り、スイッチはレガシー スイッチがリンクから削除されたことを検出できません。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 gigabitethernet0/1
```

■ clear spanning-tree detected-protocols

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 vmmps statistics

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

clear vmmps 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	変更箇所
12.2(53)EX	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 メンバーシップ 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 vmmps statistics
```

情報が削除されたかどうかを確認するには、**show vmmps 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 vmmps	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。

conform-action

レートに適合バーストよりも小さくすることによって、認定情報レート (CIR) または最大情報レート (PIR) に適合するパケットのポリシーマップ クラスのアクションを複数設定するには、**conform-action** ポリシーマップ クラス ポリシング コンフィギュレーション コマンドを使用します。アクションをキャンセルしたり、デフォルト アクション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。

```
conform-action {drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit}}
```

```
no conform-action {drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit}}
```

構文の説明

drop	パケットをドロップします。
set-cos-transmit <i>new-cos-value</i>	パケットの新しいサービス クラス (CoS) 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 CoS 値に指定できる範囲は 0 ~ 7 です。
set-dscp-transmit <i>new-dscp-value</i>	パケットの新しい DiffServ コード ポイント (DSCP) 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 DSCP 値に指定できる範囲は 0 ~ 63 です。
set-prec-transmit <i>new-precedence-value</i>	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 IP precedence 値に指定できる範囲は 0 ~ 7 です。
set-qos-transmit <i>qos-group-value</i>	パケットの新しい Quality of Service (QoS) グループ値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 QoS 値に指定できる範囲は 0 ~ 99 です。
cos	(任意) 着信パケットの CoS 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
dscp	(任意) 着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
precedence	(任意) 着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
table <i>table-map name</i>	(任意) 上記の <i>from-type</i> キーワードとともに使用します。拡張パケットマーキングに使用するテーブル マップを指定します。このテーブル マップを使用して、アクションの <i>from-type</i> パラメータに基づき、アクションの <i>to-type</i> がマーキングされます。
transmit	(任意) パケットを変更せずに送信します。

デフォルト

デフォルトの適合アクションは、パケットの送信です。

コマンドモード ポリシーマップ クラス ポリシング設定

コマンド履歴	リリース	変更箇所
	12.2(53)EX	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 レートが設定されている適合バーストよりも少ない場合に、パケットの適合アクションを設定します。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。

適合アクション マーキングを設定するには、拡張パケット マーキングを使用して、任意の着信 QoS マーキングおよびテーブル マップに基づき QoS マーキングを変更します。また、スイッチは、同じクラスの複数の QoS パラメータの同時マーキングと適合アクション、超過アクション、および違反アクション マーキングをサポートします。

ポリシーマップ クラス ポリシング コンフィギュレーション モードにアクセスするには、**police** ポリシーマップ クラス コマンドを入力します。詳細については、**police** ポリシーマップ クラス コンフィギュレーション コマンドを参照してください。

トラフィック クラスに 1 つ以上の適合アクションを設定するには、このコマンドを使用します。

例 次の例は、23000 ビット/秒 (bps) の認定情報レートおよび 10000 bps の適合バースト レートを設定するポリシー マップの複数の適合アクションを設定する方法を示します。このポリシー マップには、複数の適合アクション (DSCP 用およびレイヤ 2 CoS 用) および超過アクションが含まれます。

```
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# 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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
	exceed-action	CIR を超過するトラフィックに対して実行するアクションを定義します。
	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。
	police	分類したトラフィックにポリサーを定義します。
	show policy-map	QoS ポリシー マップを表示します。
	violate-action	適合レートに超過バーストを加えたレートよりも大きいレートのトラフィックで実行されるアクションを定義します。

copy logging onboard module

オンボード障害ロギング (OBFL) データをローカル ネットワークまたは特定のファイル システムにコピーするには **copy logging onboard module** 特権 EXEC コマンドを使用します。

copy logging onboard module *[slot-number] destination*

構文の説明

<i>slot-number</i>	(任意) スロット番号は常に 1 で、CGS 2520 には関連しません。
<i>destination</i>	ローカル ネットワーク上またはファイル システム上にある、システム メッセージのコピー先とする場所を指定します。 <i>destination</i> には、ローカルまたはネットワーク ファイル システム上のコピー先の場所とファイル名を指定します。次のオプションがサポートされています。 <ul style="list-style-type: none"> ローカル フラッシュ ファイル システムの構文： flash:/filename FTP の構文： ftp://username:password@host/filename HTTP サーバの構文： http://[[username:password]@]{hostname host-ip}[/directory]/filename null ファイル システムの構文： null:/filename NVRAM の構文： nvramp:/filename Remote Copy Protocol (RCP) の構文：rcp://username@host/filename スイッチ ファイル システムの構文： system:/filename TFTP の構文： tftp://[location]/directory/filename 一時ファイル システムの構文： tmpsys:/filename

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

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

OBFL については、**hw-module module logging onboard** 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。

例 次の例は、フラッシュ ファイル システムの *obfl_file* ファイルに OBFL データ メッセージをコピーする方法を示します。

```
Switch# copy logging onboard module flash:obfl_file
OBFL copy successful
```

関連コマンド

コマンド	説明
hw-module module logging onboard	OBFL をイネーブルにします。
show logging onboard	OBFL 情報を表示します。

cpu traffic qos cos

コントロールプレーントラフィックのサービスクラス (CoS) に基づいて Quality of Service (QoS) マーキングを設定するには、グローバルコンフィギュレーションモードで **cpu traffic qos cos** 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。

```
cpu traffic qos cos {cos_value | cos [table-map table-map-name] | dscp [table-map
table-map-name] | precedence [table-map table-map-name]}
```

```
no cpu traffic qos cos {cos_value | cos [table-map table-map-name] | dscp [table-map
table-map-name] | precedence [table-map table-map-name]}
```

構文の説明

<i>cos-value</i>	CoS 値を指定します。指定できる範囲は 0 ~ 7 です。CoS 値が設定されていない場合、各パケットのプロトコル固有のデフォルト値が適用されます。
cos	テーブルマップを使用して、パケットの CoS 値に基づく CoS 値を設定します。
table-map <i>table-map-name</i>	パケットの CoS 値に基づく CPU トラフィック CoS のマーキングに使用するテーブルマップを指定します。
dscp	テーブルマップを使用して、パケットの DSCP 値に基づく CoS 値を設定します。
table-map <i>table-map-name</i>	パケットの DSCP 値に基づく CPU トラフィック CoS のマーキングに使用するテーブルマップを指定します。
precedence	precedence 値を設定します。指定できる範囲は 0 ~ 7 です。
table-map <i>table-map-name</i>	パケットの IP-precedence 値に基づく CPU トラフィック CoS のマーキングに使用するテーブルマップを指定します。

コマンドデフォルト

コントロールプレーン (CPU) トラフィックは QoS ではマーキングされません。

コマンドモード

グローバルコンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

必要なテーブルマップを設定してから、CPU トラフィックのマーキングまたはキューイングを設定します。

この機能はスイッチでグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。

個別の回線上でそれぞれ **cpu traffic qos** マーキングアクションを入力します。

cpu traffic qos cos グローバルコンフィギュレーションコマンドは、特定の CoS 値またはテーブルマップの両方ではなく、いずれかを使用して、CPU 生成トラフィックの CoS マーキングを設定します。新しく設定を行うと、既存の設定は置き換えられます。

cpu traffic qos cos グローバル コンフィギュレーション コマンドがテーブル マップで設定されている場合、一度に2つの **map from** 値 (CoS と DSCP または precedence のいずれか) を設定できます。

cpu traffic qos cos グローバル コンフィギュレーション コマンドが IP-DSCP または IP-precedence の **map from** 値だけで設定されている場合、次のようになります。

- IP パケットの CoS 値は、パケットの IP-DSCP (または IP-precedence) 値および設定されたテーブル マップを使用してマッピングされます。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- 非 IP パケットの CoS 値は変わりません。

cpu traffic qos cos グローバル コンフィギュレーション コマンドが CoS の **map from** 値で設定されている場合、次のようになります。

- IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- 非 IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

cpu traffic qos cos グローバル コンフィギュレーション コマンドが DSCP または precedence および CoS の **map from** 値で設定されている場合、次のようになります。

- IP パケットの CoS 値は、パケットの DSCP または precedence 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。
- 非 IP パケットの CoS 値は、パケットの CoS 値および設定されたテーブル マップを使用してマッピングされています。パケットは、マーキングされた CoS 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

例

次に、パケットの DSCP 値に基づいて CPU 生成 IP トラフィック (IP-SLA および TWAMP を含む) の CoS をマーキングし、CoS 値に基づいて出力キューイングを設定する例を示します。

この設定例の結果は次のとおりです。

- CPU によって生成されたすべての IP トラフィックは、DSCP 値および *output-policy* という設定済み出力ポリシー マップに基づいて出力ポートのキューに格納される。
- 音声トラフィックをシミュレートする DSCP 値が *ef* のすべての IP SLA または TWAMP プロープが *voice* クラスに割り当てられている。
- 音声トラフィックをシミュレートする DSCP 値が *af41*、*af42* および *af43* のすべての IP SLA または TWAMP が *video* クラスに割り当てられている。
- DSCP 値が 48 および 56 のすべての IP 制御プロトコルトラフィックが *network-internetwork-control* クラスに割り当てられている。
- 残りの IP トラフィックがデフォルトクラスに割り当てられている。
- CoS 5 のすべての CPU 生成非 IP トラフィックが *voice* クラスに割り当てられている。
- CoS 3 のすべての CPU 生成非 IP トラフィックが *video* クラスに割り当てられている。
- CoS 6 および 7 のすべての CPU 生成非 IP トラフィックが *network-internetwork-control* クラスに割り当てられている。
- CoS 5 のすべての CFM トラフィックが *voice* クラスに割り当てられている。
- CoS 3 のすべての CFM トラフィックが *video* クラスに割り当てられている。

- CoS 6 および 7 のすべての CFM トラフィックが *network-internetnetwork-control* クラスに割り当てられている。

テーブル マップ :

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# map from af41 to 3
Switch(config-tablemap)# map from af42 to 3
Switch(config-tablemap)# map from af43 to 3
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

CPU QoS :

```
Switch(config)# cpu traffic qos cos dscp table-map dscp-to-cos
Switch(config)# cpu traffic qos cos cos
```

クラス :

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any network-internetnetwork-control
Switch(config-cmap)# match cos 6 7
Switch(config-cmap)# exit
```

ポリシー :

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class network-internetnetwork-control
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

インターフェイス

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos dscp	コントロールプレーン トラフィックの DSCP に基づく Quality of Service (QoS) マーキングを設定します。
cpu traffic qos precedence	コントロールプレーン トラフィックの優先順位に基づく Quality of Service (QoS) マーキングを設定します。
cpu traffic qos qos-group	サービス クラス (CoS)、IP DiffServ コード ポイント (DSCP)、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成 トラフィックを出力ポリシーマップの 1 つのクラスにマッピングします。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 cpu traffic qos	CPU トラフィックに設定される QoS マーキングを表示します。
show policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示 します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約 ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報 を表示します。
table-map	Quality of Service (QoS) マッピングを設定し、テーブルマップ コンフィ ェギュレーション モードを開始します。

cpu traffic qos dscp

コントロールプレーントラフィックの DiffServ コードポイント (DSCP) 値に基づいて Quality of Service (QoS) マーキングを設定するには、グローバルコンフィギュレーションモードで **cpu traffic qos dscp** 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。

```
cpu traffic qos dscp {dscp_value | cos [table-map table-map-name] | dscp [table-map table-map-name] | precedence [table-map table-map-name]}
```

```
no cpu traffic qos dscp {dscp_value | cos [table-map table-map-name] | dscp [table-map table-map-name] | precedence [table-map table-map-name]}
```

構文の説明

<i>dscp-value</i>	IP-DSCP 値を指定します。指定できる範囲は 0 ~ 63 です。IP-DSCP 値が設定されていない場合、各パケットのプロトコル固有のデフォルト値が適用されます。
cos	テーブルマップを使用して、パケットの IP-DSCP 値に基づく CoS 値を設定します。
table-map <i>table-map-name</i>	パケットの CoS 値に基づく CPU トラフィック IP-DSCP のマーキングに使用するテーブルマップを指定します。
dscp	テーブルマップを使用して、パケットの IP-DSCP に基づく IP-DSCP 値を設定します。
table-map <i>table-map-name</i>	パケットの IP-DSCP 値に基づく CPU トラフィック IP-DSCP のマーキングに使用するテーブルマップを指定します。
precedence	テーブルマップを使用して、パケットの IP-precedence 値に基づく IP-precedence 値を設定します。
table-map <i>table-map-name</i>	パケットの IP-precedence 値に基づく CPU トラフィック IP-DSCP 値のマーキングに使用するテーブルマップを指定します。

コマンドデフォルト

コントロールプレーン (CPU) トラフィックは QoS ではマーキングされません。

コマンドモード

グローバルコンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この機能はスイッチでグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。

個別の回線上でそれぞれ **cpu traffic qos** マーキングアクションを入力します。

cpu traffic qos dscp グローバルコンフィギュレーションコマンドは、特定の DSCP 値またはテーブルマップの両方ではなく、いずれかを使用して、CPU 生成 IP トラフィックの IP-DSCP マーキングを設定します。新しく設定を行うと、既存の設定は置き換えられます。

cpu traffic qos dscp グローバル コンフィギュレーション コマンドと **cpu traffic qos precedence** グローバル コンフィギュレーション コマンドは相互に排他的です。新しく設定を行うと、既存の設定は置き換えられます。

cpu traffic qos dscp グローバル コンフィギュレーション コマンドがテーブル マップで設定されている場合、一度に1つの **map from** 値 (DSCP、precedence、または CoS) しか設定できません。新しく設定を行うと、既存の設定は置き換えられます。このコマンドでマーキングされたパケットは、マーキングされた DSCP 値または precedence 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

DSCP および precedence 両方の **map from** 値は設定できません。新しく設定を行うと、既存の設定は置き換えられます。

例

次に、CPU 生成 IP パケットの DSCP 値に基づいて出力キューイングを設定する例を示します。

この設定例の結果は次のとおりです。

- IP DSCP 値および設定済み出力ポリシー マップ *output-policy* に基づく、出力ポート上のすべての CPU 生成 IP トラフィック キュー。
- 音声トラフィックをシミュレートする DSCP 値が *ef* のすべての IP SLA または TWAMP プロープが *voice* クラスに割り当てられている。
- 音声トラフィックをシミュレートする DSCP 値が *af41*、*af42* および *af43* のすべての IP SLA または TWAMP が *video* クラスに割り当てられている。
- DSCP 値が *48* および *56* のすべての IP 制御プロトコル トラフィックが *network-internetnetwork-control* クラスに割り当てられている。
- 残りの IP トラフィックがデフォルト クラスに割り当てられている。
- すべての CPU 生成非 IP トラフィックが、スタティックに出力ポートの固定キューにマッピングされている。
- CoS に基づくクラスが存在しないため、すべての CFM トラフィックがデフォルト クラスにキューイングされている。

```
Switch(config)# cpu traffic qos dscp dscp
```

クラス :

```
Switch(config)# class-map match-any video  
Switch(config-cmap)# match ip dscp af41 af42 af43  
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any voice  
Switch(config-cmap)# match ip dscp ef  
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any network-internetnetwork-control  
Switch(config-cmap)# match ip dscp 48 56  
Switch(config-cmap)# exit
```

ポリシー :

```
Switch(config)# policy-map output-policy  
Switch(config-pmap)# class voice  
Switch(config-pmap-c)# priority  
Switch(config-pmap-c)# police cir 10000000  
Switch(config-pmap-c)# exit  
Switch(config-pmap)# class video  
Switch(config-pmap-c)# bandwidth percent 40  
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap) # class network-internet-control
Switch(config-pmap-c) # bandwidth percent 10
Switch(config-pmap-c) # exit
Switch(config-pmap) # class class-default
Switch(config-pmap-c) # bandwidth percent 30
Switch(config-pmap-c) # exit
```

インターフェイス

```
Switch(config) # interface fastethernet0/1
Switch(config-if) # service-policy output output-policy
Switch(config-pmap-c) # exit
```

次の例を示します。

- パケットの DSCP 値に基づいて CPU 生成 IP トラフィック (IP-SLA および TWAMP を含む) の DSCP 値をマーキングする。
- パケットの DSCP 値に基づいて CPU 生成 IP トラフィック (IP-SLA および TWAMP を含む) の CoS をマーキングする。
- パケットの CoS 値に基づいて CPU 生成非 IP トラフィックの CoS をマーキングする。
- QoS グループが付いたすべての CPU 生成トラフィックをマーキングする。
- QoS グループに基づいて出力キューイングを設定する。

この例の結果は次のとおりです。

- DSCP 値が 46、48、および 56 のすべての CPU 生成 IP トラフィックでは、既存のマーキングが維持される。
- その他のすべての CPU 生成 IP パケットについては、DSCP 値は 0 にリセットされる。
- DSCP 値が 46、48、および 56 のすべての CPU 生成 IP トラフィックは、それぞれ対応する CoS 値 5、6、および 7 にマッピングされる。
- その他のすべての CPU 生成 IP パケットについては、CoS 値は 0 にリセットされる。
- CoS 値が 5、6、および 7 のすべての CPU 生成非 IP トラフィックでは、既存のマーキングが維持される。
- その他のすべての CPU 生成非 IP パケットについては、CoS 値は 0 にリセットされる。
- すべての CPU 生成トラフィックは、*cpu-traffic* という 1 つのクラスを通過する。*user-voice* クラスである *user-voice* および *user-video* は、ユーザトラフィック用に確保されています。その結果、CPU トラフィックおよびユーザトラフィックは出力ポートのさまざまなキューに分割されています。

テーブルマップ

```
Switch(config) # table-map dscp-to-cos
Switch(config-tablemap) # map from 46 to 5
Switch(config-tablemap) # map from 48 to 6
Switch(config-tablemap) # map from 56 to 7
Switch(config-tablemap) # default 0
Switch(config-tablemap) # end
```

```
Switch(config) # table-map dscp-to-dscp
Switch(config-tablemap) # map from 46 to 46
Switch(config-tablemap) # map from 48 to 48
Switch(config-tablemap) # map from 56 to 56
Switch(config-tablemap) # default 0
Switch(config-tablemap) # end
```

```
Switch(config)# table-map cos-to-cos
Switch(config-tablemap)# map from 5 to 5
Switch(config-tablemap)# map from 6 to 6
Switch(config-tablemap)# map from 7 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

CPU QoS :

```
Switch(config)# cpu traffic qos dscp dscp table-map dscp-to-dscp
Switch(config)# cpu traffic qos cos dscp table dscp-to-cos
Switch(config)# cpu traffic qos cos cos table cos-to-cos
Switch(config)# cpu traffic qos qos-group 50
```

クラス :

```
Switch(config)# class-map match-any cpu-traffic
Switch(config-cmap)# match qos-group 50
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any user-video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any user-voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

ポリシー :

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class user-voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class user-video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cpu-traffic
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

インターフェイス :

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos cos	コントロールプレーン トラフィックのサービス クラス (CoS) マーキングを設定します。
cpu traffic qos precedence	コントロールプレーン トラフィックの優先順位に基づく Quality of Service (QoS) マーキングを設定します。

コマンド	説明
cpu traffic qos qos-group	サービス クラス (CoS)、IP DiffServ コード ポイント (DSCP)、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成トラフィックを出力ポリシーマップの 1 つのクラスにマッピングします。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 cpu traffic qos	CPU トラフィックに設定される QoS マーキングを表示します。
show policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約 ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報を表示します。
table-map	Quality of Service (QoS) マッピングを設定し、テーブルマップ コンフィギュレーション モードを開始します。

cpu traffic qos precedence

コントロールプレーントラフィックの Quality Of Service (QoS) を設定するには、グローバル コンフィギュレーションモードで **cpu traffic qos precedence** 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。

```
cpu traffic qos precedence {precedence_value | cos [table-map table-map-name] | dscp
[table-map table-map-name] | precedence [table-map table-map-name]}
```

```
no cpu traffic qos precedence {precedence_value | cos [table-map table-map-name] | dscp
[table-map table-map-name] | precedence [table-map table-map-name]}
```

構文の説明

<i>precedence-value</i>	precedence 値を設定します。指定できる範囲は 0 ~ 7 です。IP-precedence 値が設定されていない場合、各パケットのプロトコル固有のデフォルト値が適用されます。 (注) 次のキーワードを 0 ~ 7 の数字に置き換えることができます。 <ul style="list-style-type: none"> • routine (0) • priority (1) • immediate (2) • flash (3) • flash-override (4) • critical (5) • internet (6) • network (7)
cos	テーブルマップを使用して、パケットの CoS 値に基づく CoS 値を設定します。
table-map <i>table-map-name</i>	パケットの CoS 値に基づく CPU トラフィック CoS のマーキングに使用するテーブルマップを指定します。
dscp	テーブルマップを使用して、パケットの IP-DSCP 値に基づく DiffServ コードポイント (DSCP) 値を設定します。
table-map <i>table-map-name</i>	パケットの DSCP 値に基づく CPU トラフィック precedence のマーキングに使用するテーブルマップを指定します。
precedence	テーブルマップを使用して、パケットの IP-precedence 値に基づく IP-precedence 値を設定します。
table-map <i>table-map-name</i>	パケットの precedence 値に基づく CPU トラフィック precedence のマーキングに使用するテーブルマップを指定します

コマンドデフォルト

コントロールプレーン (CPU) トラフィックは QoS ではマーキングされません。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この機能はスイッチでグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。

個別の回線上でそれぞれ **cpu traffic qos** マーキングアクションを入力します。

cpu traffic qos dscp グローバル コンフィギュレーション コマンドと **cpu traffic qos precedence** グローバル コンフィギュレーション コマンドは相互に排他的です。新しく設定を行うと、既存の設定は置き換えられます。

cpu traffic qos precedence グローバル コンフィギュレーション コマンドがテーブルマップで設定されている場合、一度に 1 つの **map from** 値 (DSCP、precedence、または CoS) しか設定できません。新しく設定を行うと、既存の設定は置き換えられます。このコマンドでマーキングされたパケットは、マーキングされた precedence 値または DSCP 値に基づいて、出力ポリシー マップで分類し、キューイングできます。

DSCP および precedence 両方の **map from** 値は設定できません。新しく設定を行うと、既存の設定は置き換えられます。

例

次の例は、DSCP 値に基づいて precedence をマーキングし、precedence 値に基づいて出力キューイングを設定する方法を示します。

この例の結果は次のとおりです。

- DSCP 値が 48 の CPU 生成 IP トラフィックが precedence 値 7 にマーキングされる。
- その他の CPU 生成 IP トラフィックが precedence 値 0 にマーキングされる。
- その他すべての CPU 生成非 IP トラフィックがデフォルト クラスによって処理される。
- クラスの優先順位 7 を使用して precedence 値 7 の CPU 生成 IP トラフィックがキューに格納される。
- その他すべての CPU 生成 IP トラフィックがデフォルト クラスによって処理される。

テーブルマップ:

```
switch(config)# table-map dscp-to-prec
switch(config-tablemap)# map from 48 to 7
switch(config-tablemap)# default 0
switch(config-tablemap)# end
```

CPU QoS

```
switch(config)# cpu traffic qos precedence dscp table-map dscp-to-prec
```

クラスマップ:

```
switch(config)# class-map prec7
switch(config-cmap)# match ip precedence 7
switch(config-cmap)# end
```

ポリシーマップ:

```
switch(config)# policy-map output-policy
switch(config-pmap)# class prec7
switch(config-pmap-c)# priority
switch(config-pmap-c)# end
```

インターフェイス :

```
switch(config)# interface g1/0/1
switch(config-if)# service-policy output output-policy
switch(config-if)# exit
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos cos	コントロールプレーン トラフィックのサービス クラス (CoS) マーキングを設定します。
cpu traffic qos dscp	コントロールプレーン トラフィックの DSCP に基づく Quality of Service (QoS) マーキングを設定します。
cpu traffic qos qos-group	サービス クラス (CoS)、IP DiffServ コードポイント (DSCP)、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成トラフィックを出力ポリシーマップの 1 つのクラスにマッピングします。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 cpu traffic qos	CPU トラフィックに設定される QoS マーキングを表示します。
show policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報を表示します。
table-map	Quality of Service (QoS) マッピングを設定し、テーブルマップ コンフィギュレーション モードを開始します。

cpu traffic qos qos-group

サービス クラス (CoS)、IP DiffServ コード ポイント (DSCP)、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成トラフィックを出力ポリシーマップの 1 つのクラスにマッピングするには、グローバル コンフィギュレーション モードで **cpu traffic qos qos-group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cpu traffic qos qos-group qos-group-value

no cpu traffic qos qos-group qos-group-value

構文の説明

qos-group-value QoS グループ番号を指定します。有効な値は 0 ~ 99 です。

コマンド デフォルト

コントロールプレーン (CPU) トラフィックは QoS ではマーキングされません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

この機能はスイッチでグローバルに設定する必要があります。ポート単位またはプロトコル単位では設定できません。

個別の回線上でそれぞれ **cpu traffic qos** マーキング アクションを入力します。

cpu traffic qos qos-group グローバル コンフィギュレーション コマンドを使用して、特定の QoS グループの CPU 生成トラフィックだけの QoS グループ マーキングを設定できます。table-map オプションは使用できません。

例

次の例は、すべての CPU 生成トラフィックを QoS グループでマーキングし、その QoS グループに基づいて出力キューイングを設定する方法を示します。

CPU QoS

```
switch(config)# cpu traffic qos qos-group 40
```

クラスマップ:

```
switch(config)# class-map group40
switch(config-cmap)# match qos-group 40
switch(config-cmap)# end
```

ポリシーマップ:

```
switch(config)# policy-map output-policy
switch(config-pmap)# class group40
switch(config-pmap-c)# bandwidth percent 50
switch(config-pmap-c)# end
```

インターフェイス :

```
Switch(config)# interface g1/0/1
Switch(config-if)# service-policy output output-policy
Switch(config-if)# exit
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos cos	コントロールプレーン トラフィックのサービス クラス (CoS) マーキングを設定します。
cpu traffic qos dscp	コントロールプレーン トラフィックの DSCP に基づく Quality of Service (QoS) マーキングを設定します。
cpu traffic qos precedence	コントロールプレーン トラフィックの優先順位に基づく Quality of Service (QoS) マーキングを設定します。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 cpu traffic qos	CPU トラフィックに設定される QoS マーキングを表示します。
show policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情報を表示します。
table-map	Quality of Service (QoS) マッピングを設定し、テーブルマップ コンフィギュレーション モードを開始します。

define interface-range

インターフェイス範囲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

<i>macro-name</i>	インターフェイス範囲マクロの名前（最大 32 文字）
<i>interface-range</i>	インターフェイス範囲。インターフェイス範囲の有効な値については、「使用上のガイドライン」を参照してください。

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	変更箇所
12.2(53)EX	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、**gabitethernet 0/1 - 2** であれば範囲は指定されますが、**gigabitethernet 0/1-2** では指定されません。

type および *interface* の有効値は次のとおりです。

- **vlan *vlan-id***。ここで、*vlan-id* の範囲は 1 ~ 4094 です。
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 *module*/{*first port*} - {*last port*}**

- **gigabitethernet** *module*/{*first port*} - {*last port*}

物理インターフェイス

- モジュールは常に 0 です。
- 指定できる範囲は、*type 0/number - number* です (例 : **gigabitethernet 0/1 - 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。

gigabitethernet0/1 - 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。

fastethernet0/3, gigabitethernet0/1 - 2

fastethernet0/3 -4, gigabitethernet0/1 - 2

例

次の例では、複数インターフェイスのマクロを作成する方法を示します。

```
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

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。 ローカル フラッシュ ファイル システムの構文： flash:
/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	変更箇所
12.2(53)EX	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; アクセス コントロール 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。

```
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。
<i>sender-ip sender-ip-mask</i>	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。
<i>sender-mac sender-mac-mask</i>	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。
<i>target-ip target-ip-mask</i>	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。
<i>target-mac target-mac-mask</i>	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

deny (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	変更箇所
12.2(53)EX	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 Access Control List (ACL; アクセス コントロール リスト) 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 リストの拒否条件を設定するには、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] [routing] [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] [routing] [sequence value] [time-range name]
```

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] [routing] [sequence value] [time-range  
name]
```

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]  
[routing] [sequence value] [syn] [time-range name] [urg]
```

ユーザ データグラム プロトコル

```
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}] [routing] [sequence value] [time-range  
name]
```



(注)

このコマンドは、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

構文の説明

<i>protocol</i>	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。
<i>source-ipv6-prefix/prefix-length</i>	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。
any	IPv6 プレフィクス :::0 の省略形。
host <i>source-ipv6-address</i>	拒否条件を設定する送信元 IPv6 ホスト アドレス。 この <i>source-ipv6-address</i> 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。
<i>operator</i> [<i>port-number</i>]	(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。 <i>source-ipv6-prefix/prefix-length</i> 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。 <i>destination-ipv6-prefix/prefix-length</i> 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 <i>port-number</i> 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。
<i>destination-ipv6-prefix/prefix-length</i>	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。
host <i>destination-ipv6-address</i>	拒否条件を設定する宛先 IPv6 ホスト アドレス。 この <i>destination-ipv6-address</i> 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 <i>value</i>	(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 DiffServ コード ポイント値を照合します。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 <i>operator</i> [<i>port-number</i>] 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が、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。
routing	(任意) ルーティング拡張ヘッダーを持つパケットをマッチングします。
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には照合しません。
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は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。

deny (IPv6 アクセス リスト コンフィギュレーション)

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	変更箇所
	12.2(53)EX	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、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が、IPv6 固有です。

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 ネイバー探索を許可します。ICMPv6 ネイバー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。3 つの暗黙的な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 ネイバー探索プロセスでは、IPv6 ネットワーク層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 ネイバー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 ネイバー探索プロセスと同等の Address Resolution Protocol (ARP) は、別のデータリンク層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 (*source* プレフィクスは、ソースに基づいてトラフィックをフィルタリングします。*destination* プレフィクスは、宛先に基づいてトラフィックをフィルタリングします)。

このスイッチは、すべての範囲のプレフィクス長で IPv6 アドレス マッチングをサポートしています。

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。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。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。最初の許可エントリは、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。2 番目の許可エントリは、その他すべてのトラフィックがインターフェイスで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 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 gigabitethernet0/2
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。
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 トラフィックが転送されないようにするには、**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 | larc-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 | larc-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 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。 <i>type</i> には、0 ~ 65535 の 16 進数を指定できます。 <i>mask</i> は、照合を行う前に Ethertype に適用される <i>don't care</i> 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。
larc-sca	(任意) EtherType DEC-LARC-SCA を選択します。

lsap <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と IEEE 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。 <i>mask</i> は、照合を行う前に LSAP 番号に適用される <i>don't care</i> 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) Echo 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tring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 2-2 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 2-2 IPX フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	フレーム タイプ	
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	変更箇所
12.2(53)EX	このコマンドが追加されました。

deny (MAC アクセス リスト コンフィギュレーション)

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。**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; アクセス コントロール エントリ) 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。



(注)

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

ヘルス モニタリング診断テストを設定するには、**diagnostic monitor** グローバル コンフィギュレーション コマンドを使用します。テストをディセーブルにし、デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

diagnostic monitor interval test {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds*
day

diagnostic monitor test {*name* | *test-id* | *test-id-range* | **all**}

diagnostic monitor syslog

diagnostic monitor threshold test {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count*

no diagnostic monitor interval test {*name* | *test-id* | *test-id-range* | **all**}

no diagnostic monitor test {*name* | *test-id* | *test-id-range* | **all**}

no diagnostic monitor syslog

no diagnostic monitor threshold test {*name* | *test-id* | *test-id-range* | **all**} **failure count**
count

構文の説明

interval test	テストの間隔を設定します。
test	実行するテストを指定します。
<i>name</i>	テスト名を指定します。テスト ID のリストのテスト名を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
<i>test-id</i>	テストの ID 番号を指定します。指定できる範囲は 1 ~ 6 です。テスト ID のリストのテスト番号を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
<i>test-id-range</i>	複数のテストをテストの ID 番号の範囲で指定します。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）。テスト ID のリストのテスト番号を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
all	すべての診断テストを指定します。
<i>hh:mm:ss</i>	モニタリング間隔を時、分、秒で設定します。 <ul style="list-style-type: none"> • <i>hh</i> : 時間 (0 ~ 24) を入力します。 • <i>mm</i> : 分 (0 ~ 60) を入力します。 • <i>ss</i> : 秒 (0 ~ 60) を入力します。
<i>milliseconds</i>	モニタリング間隔 (テスト時間) をミリ秒 (ms) 単位で設定します。指定できる範囲は 0 ~ 999 ミリ秒です。
<i>day</i>	モニタリング間隔をテストとテストの間の日数で設定します。指定できる範囲は 0 ~ 20 日です。
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 test	障害しきい値を設定します。
failure count <i>count</i>	障害しきい値のカウントを設定します。 <i>count</i> に指定できる範囲は 0 ~ 99 です。

■ diagnostic monitor

デフォルト

モニタリングはディセーブルで、障害しきい値は設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

- 診断モニタリングをイネーブルにする前に、障害しきい値およびテストの間隔を設定する必要があります。
- 診断モニタリングイネーブルにするには、**diagnostic monitor test 1** コマンドを入力します。
- **diagnostic monitor test {name | test-id | test-id-range | all}** コマンドを入力する場合は、接続されているすべてのポートをディセーブルにしてネットワークトラフィックを分離する必要があります。
- テスト中はテストパケットを送信しないでください。

例

次に、ヘルス モニタリング テストを設定する例を示します。

```
Switch(config)# diagnostic monitor threshold test 1 failure count 20
Switch(config)# diagnostic monitor interval test 1 12:30:00 750 5
```

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 test

診断テストのスケジュールを設定するには、**diagnostic schedule test** 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。スケジュー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。

diagnostic schedule test {*name* | *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 test {*name* | *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

name	テスト名を指定します。テスト ID のリストのテスト名を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
test-id	テストの ID 番号を指定します。指定できる範囲は 1 ~ 6 です。テスト ID のリストのテスト番号を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
test-id-range	複数のテストをテストの ID 番号の範囲で指定します。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)。テスト ID のリストのテスト番号を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
all	すべての診断テストを指定します。
basic	基本的なオンデマンドの診断テストを指定します。
non-disruptive	ノンディスラプティブヘルス モニタリング テストを指定します。
daily <i>hh:mm</i>	診断テストのスケジュールリング (日単位) を指定します。 <i>hh:mm</i> : 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 (例: 12:30)。
on <i>mm dd yyyy</i> <i>hh:mm</i>	特定の日時の診断テストのスケジュールリングを指定します。 <i>mm dd yyyy</i> : <ul style="list-style-type: none"> <i>mm</i> : January、February のように、月を大文字または小文字で入力します。 <i>dd</i> : 2 桁の数字で日を入力します (例: 03、16)。 <i>yyyy</i> : 4 桁の数字で年を入力します (例: 2008)。
weekly <i>day-of-week</i> <i>hh:mm</i>	診断テストのスケジュールリング (週単位) を指定します。 <i>day-of-week</i> : Monday、Tuesday のように、曜日を大文字または小文字で入力します。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

■ diagnostic schedule test

例 次に、特定の日に診断テストをスケジュールリングする例を示します。

```
Switch(config)# diagnostic schedule test 1,2,4-6 on november 3 2006 23:10
```

次に、毎週特定の時間に診断テストを行うようスケジュールリングする例を示します。

```
Switch(config)# diagnostic schedule test TestPortAsicMem 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 test

オンライン診断テストを実行するには、**diagnostic start test** 特権 EXEC コマンドを使用します。

diagnostic start test {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**}

構文の説明

<i>name</i>	テスト名を指定します。テスト ID のリストのテスト名を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
<i>test-id</i>	テストの ID 番号を指定します。指定できる範囲は 1 ~ 6 です。テスト ID のリストのテスト番号を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
<i>test-id-range</i>	複数のテストをテストの ID 番号の範囲で指定します。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）。テスト ID のリストのテスト番号を表示するには、 show diagnostic content 特権 EXEC コマンドを入力します。
all	すべての診断テストを指定します。
basic	基本的なオンデマンドの診断テストを指定します。
non-disruptive	ノンディスラプティブヘルス モニタリング テストを指定します。

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

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

diagnostic start コマンドを使用してテストを開始したら、テスト プロセスの停止はできません。

スイッチは、次のテストをサポートしています。

ID	Test Name [On-Demand Test Attributes]
1	TestPortAsicStackPortLoopback [B*N****]
2	TestPortAsicLoopback [B*D*R**]
3	TestPortAsicCam [B*D*R**]
4	TestPortAsicRingLoopback [B*D*R**]
5	TestMicRingLoopback [B*D*R**]
6	TestPortAsicMem [B*D*R**]

テスト名を確認するには、**show diagnostic content** 特権 EXEC コマンドを使用してテスト ID リストを表示します。テスト名を使用してテスト 3 を指定するには、**diagnostic start switch number test TestPortAsicCam** 特権 EXEC コマンドを入力します。

■ diagnostic start test

複数のテストを指定するには、*test-id-range* パラメータを使用し、カンマとハイフンで区切られた整数を入力します。たとえば、テスト 2、3、および 4 を指定するには、**diagnostic start test 2-4** コマンドを入力します。テスト 1、3、4、5、および 6 を指定するには、**diagnostic start test 1,3-6** コマンドを入力します。

例

次に、診断テスト 1 を開始する例を示します。

```
Switch# diagnostic start test 1
Switch#
06:27:50: %DIAG-6-TEST_RUNNING: Running TestPortAsicStackPortLoopback{ID=1} ...
06:27:51: %DIAG-6-TEST_OK: TestPortAsicStackPortLoopback{ID=1} has completed
successfully
```

次に、診断テスト 2 を開始する例を示します。このテストを実行すると、通常システム動作が中断され、スイッチがリロードされます。

```
Switch# diagnostic start test 2
Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]: y
Switch#
00:00:25: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:29: %SYS-5-CONFIG_I: Configured from memory by console
00:00:30: %DIAG-6-TEST_RUNNING : Running TestPortAsicLoopback{ID=2} ...
00:00:30: %DIAG-6-TEST_OK: TestPortAsicLoopback{ID=2} has completed successfully
```

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 credentials

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、サブリカント 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 サブリカント 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このスイッチをサブ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、スイッチをサブ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 eapol (グローバル コンフィギュレーション)

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、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、**dot1x critical eapol** 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

no dot1x critical eapol

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

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。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポートのアクセス不能認証バイパスをイネーブルにするか、またはスイッチがクリティカルなポートを割り当てるアクセス VLAN を設定するには、**authencation 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。

関連コマンド

コマンド	説明
authentication event	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。
show dot1x	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x default

設定可能な 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 ステータス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	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例では、ポート上の設定可能な 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 guest-vlan supplicant

スイッチでオプションの IEEE 802.1x ゲスト VLAN 動作をグローバルに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。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 supplicant

no dot1x guest-vlan supplicant

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

ゲスト VLAN 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチのゲスト VLAN を設定する方法については、**authentication event no-response action authorize vlan *vlan-id*** インターフェイス コンフィギュレーション コマンドを参照してください。

例

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
```

関連コマンド

コマンド	説明
authentication event	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 authentication [interface <i>interface-id</i>]	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タスに戻すには、**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 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	変更箇所
	12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン	<p>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。</p> <p>このコマンドの no 形式はありません。</p>
------------	---

例	<p>次の例では、ポートを手動で初期化する方法を示します。</p> <pre>Switch# dot1x initialize interface gigabitethernet0/2</pre>
---	--

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 max-reauth-req

ポートが無許可ステートに移行するまでスイッチが認証プロセスを再起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

<i>count</i>	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は、2 回の再認証試行後にポートはデフォルトでゲスト VLAN で許可されます。指定できる範囲は 1 ~ 10 です。デフォルトは 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	変更箇所
12.2(53)EX	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)。
authentication timer	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。

コマンド	説明
show authentication	指定されたポートの認証ステータスを表示します。
show dot1x [interface <i>interface-id</i>]	指定されたポートの 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起動する前に、拡張認証プロトコル (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

<i>count</i>	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、認証プロセス中にサブクライアントに問題が発生した場合、オーセンティケータがデータ要求を 2 回再送信し、応答がなければプロセスを中止します。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	変更箇所
12.2(53)EX	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
authentication timer	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 authentication	指定されたポートの認証ステータスを表示します。

dot1x pae

IEEE 802.1x ポート アクセス エンティティ (PAE) タイプを設定するには、**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。設定されている PAE タイプ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

dot1x pae [supplicant | authenticator | both]

no dot1x pae [supplicant | authenticator | both]

構文の説明

supplicant	(任意) インターフェイスは、IEEE 802.1x サプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。
authenticator	(任意) インターフェイスは、IEEE 802.1x オーセンティケータとしてだけ機能し、サプリカント向けのメッセージに応答しません。
both	(任意) インターフェイスは、IEEE 802.1x サプリカントおよび IEEE 802.1x オーセンティケータとして動作するため、すべての dot1x メッセージに応答します。

デフォルト

IEEE 802.1x PAE タイプは設定されません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

dot1x system-auth-control コマンドが設定されていない場合、**supplicant** キーワードがこのコマンドで使用できる唯一のキーワードとなります (つまり、**dot1x system-auth-control** コマンドが設定されていない場合、インターフェイスをオーセンティケータとして設定できません)。

authentication port-control インターフェイス コンフィギュレーション コマンドを入力して、ポートに IEEE 802.1x 認証を設定すると、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

次に、インターフェイスをサプリカントとして動作するように設定する例を示します。

```
Router (config-if)# dot1x pae supplicant
```

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 system-auth-control	スイッチ上で IEEE 802.1x 認証をグローバルにイネーブルにします。
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。
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 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、常にサブ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

サブ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	変更箇所
12.2(53)EX	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、サブ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、サブ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、スイッチがサブ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 サブリカントのクレデンシャルを設定します。
dot1x pae supplicant	インターフェイスがサブリカントとしてだけ機能するように設定します。

dot1x system-auth-control

IEEE 802.1x をグローバルにイネーブルにするには、**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。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 system-auth-control

no dot1x system-auth-control

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 802.1x はディセーブル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	変更箇所
12.2(53)EX	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 をグローバルにイネーブルにする前に、認証、許可、およびアカウントिंग (AAA) をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

スイッチの IEEE 802.1x をグローバルにイネーブルにする前に、IEEE 802.1x 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。

例

次の例では、スイッチで IEEE 802.1x 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
```

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
authentication port-control	ポートの認証ステータスの手動制御をイネーブルにします。
show authentication	指定されたポートの認証ステータスを表示します。

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	変更箇所
12.2(53)EX	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 <i>timeout</i>	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	<i>timeout</i>	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	変更箇所
	12.2(53)EX	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 [<i>interface interface-id</i>]	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 {auth-period seconds | held-period seconds | quiet-period seconds |
ratelimit-period seconds | reauth-period {seconds | server} | server-timeout seconds
| start-period seconds | supp-timeout seconds | tx-period seconds}
```

```
no dot1x timeout {auth-period seconds | held-period seconds | quiet-period seconds |
ratelimit-period seconds | reauth-period {seconds | server} | server-timeout seconds
| start-period seconds | supp-timeout seconds | tx-period seconds}
```

構文の説明

auth-period <i>seconds</i>	サブリカント（クライアント）がオーセンティケータからの応答（Extensible Authentication Protocol over LAN（EAPOL）-Start 以外のパケット）を何秒待機するとタイムアウトとなるかを設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
held-period <i>seconds</i>	サブリカントで保留ステートが維持される秒数（つまり、サブリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルト値は 60 です。
quiet-period <i>seconds</i>	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 <i>seconds</i>	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 { <i>seconds</i> 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。 <ul style="list-style-type: none"> 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 <i>seconds</i>	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。30 の最小設定を推奨します。
start-period <i>second</i>	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 指定できる値は 1 ～ 65535 です。デフォルトは 30 です。
supp-timeout <i>seconds</i>	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 <i>seconds</i>	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。

auth-period は 30 秒です。

held-period は 60 秒です。

quiet-period は 60 秒です。

rate-limit は 1 秒です。

reauth-period は 3600 秒です。

server-timeout は 30 秒です。

start-period は 30 秒です。

supp-timeout は 30 秒です。

tx-period は 5 秒です。

コマンドモード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

dot1x timeout 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 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、**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定期的な再認証をイネーブルにした場合のみ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。

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)# authentication periodic
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)# authentication periodic
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
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。
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。
authentication periodic	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。

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 Mb/s または 100 Mb/s で動作するインターフェイスに限る）。1000 Mb/s または 10,000 Mb/s で動作するインターフェイスに対しては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、ギガビットイーサネットポート、および 1000BASE-T 小型フォームファクタ（SFP）モジュールのデフォルトは **auto** です。

100BASE-x（-x は -BX、-FX、-FX-FE、または -LX）SFP モジュールのデフォルトは **half** 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	変更箇所
12.2(53)EX	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、1000BASE-T SFP モジュールまたは 100BASE-FX MMF SFP モジュールが SFP モジュール スロットに挿入されている場合のみ使用できます。他のすべての SFP モジュールは全二重モードだけで動作します。

1000BASE-T SFP モジュールが SFP モジュール スロットに挿入されている場合は、デュプレックスモードを **auto** または **full** に設定できます。

100BASE-FX MMF SFP モジュールが SFP モジュール スロットに挿入されている場合は、デュプレックスモードを **half** または **full** に設定できます。100BASE-FX MMF SFP モジュールでは、**auto** キーワードを使用できますが、自動ネゴシエーションがサポートされていないため、インターフェイスは半デュプレックスモード（デフォルト）になります。

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。

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。

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、再びイネーブルになる場合があります。



(注)

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 gigabitethernet0/1
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。

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 | dhcp-rate-limit | gbic-invalid |
inline-power | l2ptguard | link-flap | loopback | pagp-flap | small-frame}
```

```
no errdisable detect cause {all | arp-inspection | dhcp-rate-limit | gbic-invalid |
inline-power | l2ptguard | link-flap | pagp-flap | small-frame}
```



(注)

コマンドライン インターフェイスでは表示されますが、既存のブロードキャスト ストーム ディセーブ ル機能が小さなフレームを正しく制御できるので、**small-frame** キーワードは必要ありません。

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。
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。
gbic-invalid	無効な Gigabit Interface Converter (GBIC; ギガビット インターフェイス コンバータ) 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、無効な小型フォーム ファクタ (SFP) モジュールを意味します。
inline-power	Power over Ethernet (PoE) の errdisable 原因に対して、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 原因に対して、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; ポート集約プロトコル) フラップの errdisable 原因のエラー検出をイネーブルにします。
small-frame	スイッチでは、この機能は不要です。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

原因 (**all**、**dhcp-rate-limit** など) は、**errdisable** ステートが発生した理由です。原因がインターフェイスで検出された場合、インターフェイスは **errdisable** ステートとなり、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。

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、インターフェイスは **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、インターフェイスを手動で **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** 原因に対して **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
```

設定を確認するには、**show errdisable detect** 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 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。

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 | gbic-invalid | inline-power | l2ptguard | link-flap | loopback |
pagp-flap | psecure-violation | security-violation | small-frame | udld | unicast-flood
| vmps} | {interval interval}}
```

```
no errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | gbic-invalid | inline-power | l2ptguard | link-flap | loopback |
pagp-flap | psecure-violation | security-violation | small-frame | udld | unicast-flood
| vmps} | {interval interval}}
```



(注)

storm-control キーワードおよび **unicast-flood** キーワードはコマンドラインのヘルプ スtring に表示されますが、サポートされていません。**small-frame** キーワードは、ブロードキャスト ストーム ディセーブル機能が小さなフレームを処理するため、使用されません

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	Bridge Protocol Data Unit (BPDU; ブリッジプロトコル データ ユニット) 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。
gbic-invalid	Gigabit Interface Converter (GBIC; ギガビット インターフェイス コンバータ) 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小型フォーム ファクタ (SFP) の errdisable ステートを意味します。
inline-power	Power over Ethernet (PoE) の 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。
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; ポート集約プロトコル) 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。
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。
small-frame	このキーワードは使用されません。
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。
unicast-flood	ユニキャストフラッドディセーブル ステートから回復するタイマーをイネーブルにします。
vmmps	VLAN Membership Policy Server (VMPS; VLAN メンバーシップ 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

原因 (**all**、**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。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステート (リンクダウン ステートに類似した動作ステート) となります。その原因の errdisable 回復をイネーブルにしない場合、**shutdown** および **no shutdown** 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。原因の回復をイネーブルにした場合、インターフェイスは errdisable ステートから回復し、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します。

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、手動でインターフェイスを 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。

■ errdisable recovery

関連コマンド

コマンド	説明
show errdisable recovery	errdisable の回復タイマー情報を表示します。
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。

ethernet evc

イーサネット仮想接続 (EVC) を定義し、EVC コンフィギュレーション モードを開始するには、**ethernet evc** 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。EVC を削除するには、このコマンドの **no** 形式を使用します。

ethernet evc evc-id

no ethernet evc evc-id

構文の説明

evc-id EVC の ID。1 ~ 100 文字の文字列を設定できます。

デフォルト

EVC 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ethernet evc evc-id コマンドを入力すると、スイッチは、EVC コンフィギュレーション モードを開始して、次のコンフィギュレーション コマンドを使用できるようになります。

- **default** : EVC をデフォルト ステートに設定します。
- **exit** : EVC 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** : コマンドを無効にするか、コマンドをデフォルト設定に戻します。
- **oam protocol cfm svlan** : イーサネットの運用管理および保守 (OAM) プロトコルを IEEE 802.lag の接続障害管理 (CFM) として設定し、パラメータを設定します。 [oam protocol cfm svlan](#) コマンドを参照してください。
- **uni count** : EVC の UNI カウントを設定します。 [uni count](#) コマンドを参照してください。

例

次の例では、EVC を定義して EVC 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)# ethernet evc test1
Switch(config-etc)#
```

関連コマンド

コマンド	説明
service instance id ethernet evc-id	イーサネット サービス インスタンスを設定し、EVC を適用します。
show ethernet service evc	設定された EVC に関する情報を表示します。

ethernet lmi

イーサネット ローカル管理インターフェイス (E-LMI) としてイネーブルにする設定を行ったり、スイッチをプロバイダー エッジ (PE) デバイスまたはカスタマー エッジ (CE) デバイスとして設定したりするには、**ethernet lmi** 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。E-LMI をグローバルにディセーブルにしたり、E-LMI CE 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。

```
ethernet lmi {ce | global}
```

```
no ethernet lmi {ce | global}
```

構文の説明

ce	スイッチを E-LMI CE デバイスとしてイネーブルにします。 (注) イーサネット LMI はデフォルトでディセーブルです。E-LMI は CE モードでイネーブルにするだけでなく、グローバルにまたはインターフェイスでもイネーブルにする必要があります。
global	スイッチで E-LMI をグローバルにイネーブルにします。デフォルトでは、スイッチは PE デバイスです。

デフォルト

イーサネット LMI はディセーブルです。global キーワードを使用してイネーブルにされた場合、デフォルトでは、スイッチは PE デバイスです。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

E-LMI をグローバルにイネーブルにするには、**ethernet lmi global** コマンドを使用します。E-LMI CE デバイスとしてスイッチをイネーブルにするには、**ethernet lmi ce** コマンドを使用します。

イーサネット LMI はインターフェイスではデフォルトでディセーブルであり、**ethernet lmi interface** インターフェイス コンフィギュレーション コマンドを入力して、明示的にイネーブルにする必要があります。**ethernet lmi global** コマンドはデバイス全体のすべてのインターフェイスにおいて、PE モードでイーサネット LMI をイネーブルにします。このコマンドの利点は、各インターフェイスでイーサネット LMI を個別にイネーブルにする代わりに 1 種類のコマンドですべてのインターフェイスのイーサネット LMI をイネーブルにできることです。CE モードでインターフェイスをイネーブルにするには、**ethernet lmi ce** グローバル コンフィギュレーション コマンドも入力する必要があります。

ethernet lmi global コマンドを入力したあとで、特定のインターフェイスで E-LMI をディセーブルにするには、**no ethernet lmi interface** インターフェイス コンフィギュレーション コマンドを入力します。

ethernet lmi interface インターフェイス コンフィギュレーション コマンドと **ethernet lmi global** 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順序が重要です。入力された最新のコマンドが前のコマンドを上書きします。



(注) **ethernet lmi** インターフェイス コンフィギュレーション コマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080690f2d.html#wp1166797

スイッチを E-LMI CE デバイスとしてイネーブルにするには、**ethernet lmi global** コマンドおよび **ethernet lmi ce** コマンドの両方を入力します。デフォルトでは E-LMI はディセーブルです。E-LMI をイネーブルにしても **ethernet lmi ce** コマンドを入力しない限り、スイッチは PE モードです。

スイッチを E-LMI CE デバイスとして設定すると、次のインターフェイス コンフィギュレーション コマンドとキーワードが表示されますが、サポートされていません。

- **service instance**
- **ethernet uni**
- **ethernet lmi t392**

例

次の例では、スイッチを E-LMI CE デバイスとして設定する方法を示します。

```
Switch(config)# ethernet lmi global
Switch(config)# ethernet lmi ce
```

関連コマンド

コマンド	説明
ethernet lmi インターフェイス コンフィギュレーション コマンド	ユーザネットワーク インターフェイスの E-LMI をイネーブルにします。

ethernet lmi ce-vlan map

イーサネット ローカル管理インターフェイス (ELMI) パラメータを設定するには、**ethernet lmi ce-vlan map** のイーサネット サービス コンフィギュレーション コマンドを使用します。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ethernet lmi ce-vlan map {vlan-id | any | default | untagged}

no ethernet lmi ce-vlan map {vlan-id | any | default | untagged}

構文の説明

vlan-id	マッピングする 1 つ以上のカスタマー VLAN ID を入力します。単一の VLAN ID (範囲は 1 ~ 4094)、ハイフンで区切られた VLAN ID の範囲、またはカンマで区切った一連の VLAN ID を入力できます。
any	すべての VLAN (タグ付けされていない VLAN および 1 ~ 4094 の VLAN) をマッピングします。
default	デフォルトのサービス インスタンスにマッピングします。 default キーワードは、すでにサービス インスタンスを 1 つの VLAN または VLAN のグループにマッピングしている場合にだけ使用できます。
untagged	タグ付けされていない VLAN のみをマッピングします。

デフォルト

E-LMI マッピング パラメータは定義されていません。

コマンド モード

イーサネット サービス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	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 User-Network Interface (UNI; ユーザネットワーク インターフェイス) の E-LMI カスタマー VLAN から EVC へのマッピングを設定するには、このコマンドを使用します。

ethernet uni {bundle [all-to-one] | multiplex} 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設定されたバンドル特性に E-LMI マッピング パラメータが関連付けられます。

- デフォルト UNI 属性 (バンドルおよび多重化) の使用では、複数の EVC および複数の VLAN がサポートされます。
- ethernet uni bundle** コマンドの入力では、1 つ以上の VLAN を持つ 1 つの EVC だけがサポートされます。
- ethernet uni bundle all-to-one** コマンドの入力では、複数の VLAN がサポートされますが、EVC は 1 つだけサポートされます。**ethernet lmi ce-vlan map any** イーサネット サービス コンフィギュレーション コマンドを使用する場合、事前に **all-to-one** バンドルをインターフェイスで設定する必要があります。
- ethernet uni multiplex** コマンドの入力では、EVC ごとに VLAN を 1 つだけ持つ、複数の EVC がサポートされます。

例 次の例では、E-LMI カスタマー VLAN から EVC へのマッピングを設定し、インターフェイスのサービス インスタンス 333 にあるカスタマー VLAN 101 に EVC *test* をマッピングする方法を示します。

```
Switch(config-if)# service instance 333 ethernet test
Switch(config-if-srv)# ethernet lmi ce-vlan map 101
```

関連コマンド

コマンド	説明
<code>service instance <i>id</i> ethernet</code>	イーサネット サービス インスタンスを定義し、イーサネット サービス コンフィギュレーション モードを開始します。
<code>show ethernet service instance</code>	設定されたイーサネット サービス インスタンスに関する情報を表示します。

ethernet loopback (イーサネット コンフィギュレーション)

複数のスイッチ間での接続をテストするためのポート単位のループバックを設定するには、**ethernet loopback facility** 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。Quality of Service (QoS) をテストするには、**ethernet loopback terminal** 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。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

```
ethernet loopback facility [vlan vlan-list] [mac-address {swap | copy}] [timeout {seconds | none}] supported
```

```
ethernet loopback terminal [mac-address {swap | copy}] [timeout {seconds | none}] supported
```

```
no ethernet loopback
```

構文の説明

facility	接続テスト用のファシリティ ループバックを設定します。
vlan <i>vlan-list</i>	中断のないループバック テストの VLAN のループバックを設定します。
terminal	QoS のテストのターミナル ループバックを設定します。
mac-address swap	ループバック処理のため送信元 MAC アドレスと宛先 MAC アドレスをスワップするようスイッチを設定します。
mac-address copy	ループバック処理のため送信元 MAC アドレスと宛先 MAC アドレスをコピーするようスイッチを設定します。
timeout <i>seconds</i>	秒単位でのループバック タイムアウト時間を設定します。指定できる範囲は 5 ~ 300 秒です。デフォルトは 60 秒です。
timeout none	ループバックがタイムアウトしないように設定します。
supported	設定されたループバックをサポートするように指定します。

デフォルト

ループバックは設定されません。**mac-address** オプションが設定されていない場合、デフォルトでは、送信元アドレスおよび宛先アドレスがコピーされます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

イーサネット ループバックは、VLAN またはポート チャネルではなく、物理ポートでだけ設定できます。

ファシリティ ループバックにより、ポートでは、通常のトラフィックに対してリンクはアップ状態になりますが、ラインプロトコルはダウン状態になります。スイッチにより、すべての受信トラフィックはループバックされます。

キーワード **vlan vlan-list** を入力して VLAN ループバックを設定すると、ポートのその他の VLAN では引き続き正常にスイッチが行われるため、処理を中断させずにループバック テストできます。

ループバックは、ポートのシャットダウンやスイッチ ポートからルーテッド ポートへの変更などのポート イベント後に終了します。

ターミナル ループバックの場合、ソフトウェアでは、ポートはアップ状態であるがリンクはダウン状態であると認識され、パケットは送信されません。ポートの設定変更は、ループバックされているトラフィックに即座に影響を与えます。

ポート 1 つにつきループバックを 1 つ設定でき、スイッチ 1 つにつきループバックを 2 つまで設定できます。スイッチ 1 つにつきターミナル ループバックは 1 つだけ設定できます。そのため、スイッチには 1 つのファシリティ ループバックおよび 1 つのターミナル ループバック、または 2 つのファシリティ ループバックが存在する可能性があります。

他の機能とのイーサネット ループバックの相互作用：

- SPAN とループバックは同じスイッチで同時に設定できません。いずれかのポートにループバックが設定されている場合に任意のポートに SPAN を設定しようとする、エラー メッセージが表示されます。
- ポート ループバック機能は、VLAN マッピング機能とハードウェア リソースを共有します。ループバックを設定しようとするとき、VLAN マッピング設定のために十分な TCAM リソースが使用できない場合、エラー メッセージを受信し、設定は許可されません。
- ループバックがポート上でアクティブな場合、このポートを Flex Link ペアまたは EtherChannel に追加できません。

イーサネット ループバックを設定したら、ループバックを開始するために **ethernet loopback start interface-id** 特権 EXEC コマンドを入力します。ループバックを停止するには、**ethernet loopback stop {interface-id | all}** コマンドを入力します。

例

次に、宛先 MAC アドレスおよび送信元 MAC アドレスをスワップし、30 秒後にタイムアウトし、ループバック プロセスを開始して、設定を確認するようイーサネット ループバックを設定する方法の例を示します。設定する前に処理を確認する必要があります。

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback facility mac-address swap timeout 30 supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
This is an intrusive loopback.
Therefore, while you test Ethernet connectivity,
you will be unable to pass traffic across that link.
Proceed with Local Loopback?[confirm]
```

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface GI0/1
Direction          : facility
Type                : port
Status              : active
MAC Mode            : swap
Time out            : 30
Time remaining      : 25 seconds
```

また、2 番目のインターフェイスに中断のないループバックを設定する例を示します。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# ethernet loop facility mac-address swap timeout none supported
Switch(config-if)# exit
Switch(config-if)# interface fastethernet0/2
```

■ ethernet loopback (イーサネット コンフィギュレーション)

```
Switch(config-if)# ethernet loop facility vlan 3 mac-address copy timeout 100 supported
Switch(config-if)# switch mode trunk
Switch(config-if)# exit
switch(config)# vlan 3
switch(config-vlan)# end
```

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Fa0/1
Direction          : facility
Type                : port
Status              : configured
MAC Mode            : swap
Time out            : none
=====
Loopback Session 1 : Interface Fa0/2
Direction          : facility
Type                : vlan
Status              : configured
MAC Mode            : copy
Vlan                 : 3
Time out            : 100
```

次に、2つのインターフェイスでイーサネット ループバック機能設定を削除して、1つのインターフェイスでイーサネット ターミナル ループバックを設定する例を示します。

```
Switch(config)# interface fastethernet 0/1
switch(config-if)# no ethernet loopback
switch(config-if)# interface fastethernet 0/2
switch(config-if)# no ethernet loopback
switch(config-if)# exit
switch(config)# default interface range fastethernet 0/1-2
switch(config)# interface fastethernet 0/1
switch(config-if)# ethernet loop terminal mad-address swap timeout 300 supported
switch(config-if)# end
```

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Fa0/1
Direction          : terminal
Type                : port
Status              : configured
MAC Mode            : swap
Time out            : 300
```

■ 関連コマンド

コマンド	説明
ethernet loopback (特権 EXEC)	インターフェイス上のイーサネット ループバック操作を開始または停止します。
show ethernet loopback	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イーサネット ループバックを表示します。

ethernet loopback (特権 EXEC)

インターフェイスでイーサネット ループバック機能を開始または停止するには、**ethernet loopback** 特権 EXEC コマンドを使用します。

ethernet loopback {start interface-id | stop {interface-id | all}}

構文の説明

start	インターフェイスに設定されているイーサネット ループバック操作を開始します。
stop	イーサネット ループバック操作を停止します。
<i>interface-id</i>	ループバック操作を開始または停止するインターフェイスを指定します。
all	スイッチ上のすべてのイーサネット ループバック操作を停止します。このキーワードは、 stop キーワードの後にのみ使用できます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

イーサネット ループバック操作を開始または停止する前に、**ethernet loopback** 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、インターフェイスでイーサネット ループバックを設定する必要があります。ループバックを開始すると、警告メッセージが表示されます。

物理ポートに対してのみ、イーサネット ループバックを設定して **ethernet loopback start** コマンドまたは **ethernet loopback stop** コマンドを入力できます。VLAN やポート チャネルに対してはこれらを行うことはできません。

非トランク インターフェイスでは VLAN ループバックを開始できません。ルーテッド インターフェイスではターミナル ループバックを開始できません。

ポート 1 つにつきループバックを 1 つのみ設定でき、スイッチ 1 つにつきループバックを 2 つまで設定できます。スイッチ 1 つにつきターミナルループバックは 1 回だけ設定できます。

例

次に、ファシリティ ポート ループバック プロセスを開始し、確認して、停止する例を示します。

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback facility mac-address swap timeout 30 supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
This is an intrusive loopback.
Therefore, while you test Ethernet connectivity,
you will be unable to pass traffic across that link.
Proceed with Local Loopback?[confirm]
```

■ ethernet loopback (特権 EXEC)

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Gi0/1
Direction          : facility
Type               : port
Status             : active
MAC Mode           : swap
Time out           : 30
Time remaining     : 25 seconds

Switch# ethernet loop stop all

Dec 4 11:18:44.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Gi0/1
Direction          : facility
Type               : port
Status             : configured
MAC Mode           : swap
Time out           : 30
```

次に、VLAN の非侵入型ループバック プロセスを開始する例を示します。

```
Switch# ethernet loop start fastethernet 0/2
This is a non-intrusive loopback.
Therefore, while you test Ethernet connectivity on vlan 3, you will be unable to pass
traffic across it, however, other vlans will be unaffected.
Proceed with Local Loopback?[confirm]

Switch# show ethernet loopback
=====
Loopback Session 1 : Interface Fa0/2
Direction          : facility
Type               : vlan
Status             : active
MAC Mode           : copy
Vlan               : 3
Time out           : 100
Time remaining     : 94 seconds
```

関連コマンド

コマンド	説明
ethernet loopback (イーサネット コンフィギュレーション)	インターフェイス上のイーサネット ループバック操作を設定します。
show ethernet loopback	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イーサネット ループバックを表示します。

ethernet oam remote-failure

Ethernet Operation, administration, and Maintenance (EOM) リモート障害表示を設定するには、**ethernet oam remote-failure** インターフェイス コンフィギュレーションまたはコンフィギュレーション テンプレート コマンドを使用します。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface

no ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action

構文の説明		
critical-event		未指定のクリティカルなイベントが発生したとき、インターフェイスを errdisable モードにするようにスイッチを設定します。
dying-gasp		回復不能な状態が発生したとき、インターフェイスを errdisable モードにするようにスイッチを設定します。
link-fault		レシーバが電力の損失を検出すると errdisable モードにインターフェイスを変更するようにスイッチを設定します。

デフォルト	
	設定テンプレート インターフェイス コンフィギュレーション

コマンドモード	
	イーサネット サービス コンフィギュレーション

コマンド履歴	リリース	変更箇所
	12.2(53)EX	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、イーサネット OAM テンプレートおよびインターフェイスに適用できます。インターフェイス設定は、テンプレートの設定よりも優先されます。OAM テンプレート コンフィギュレーション モードを開始するには、**template template-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。

Cisco CGS 2520 スイッチは、Link Fault と Critical Event OAM PDU を生成しません。ただし、スイッチがこれらの PDU をリンクの相手方から受信した場合は処理します。イーサネット OAM がディセーブルのとき、インターフェイスがシャットダウンしたとき、インターフェイスが **errdisable** ステートになったとき、またはスイッチがリロードしているときに、スイッチは **Dying Gasp OAM PDU** の生成と受信をサポートします。また、スイッチは電源喪失に基づいた **Dying Gasp PDU** を生成し、受信できます。PDU には、PDU が送信された理由を示す原因コードが含まれています。リモート デバイスがディセーブルの場合、またはリモート デバイスがインターフェイス上のイーサネット OAM をディセーブルにした場合に、**errdisable** アクションを発生させるように設定できます。

イーサネット OAM プロトコルのコマンドと設定の詳細については、次の URL の Cisco IOS フィーチャ モジュールを参照してください。

http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a008067344c.html

CFM およびイーサネット OAM コマンドの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6922/products_command_reference_book09186a0080699104.html

例

次に、回復不能なエラーが発生した場合のためのリモート障害表示のイーサネット OAM テンプレート設定方法、およびインターフェイスへの適用方法の例を示します。

```
Switch(config)# template oam1
Switch(config-template)# ethernet oam remote-failure dying-gasp action error-disable interface
Switch(config-template)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# source template oam1
Switch(config-if)# exit
```

次に、回復不能なエラーが発生した場合のイーサネット OAM リモート障害表示を 1 つのインターフェイスに設定する例を示します。

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet oam remote-failure dying-gasp action error-disable interface
Switch(config-if)# exit
```

関連コマンド

コマンド	説明
show ethernet oam status [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上に設定済みのイーサネット OAM リモート障害条件を表示します。

ethernet uni

UNI バンドル属性を設定するには、**ethernet uni** 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。デフォルトのバンドル設定に戻すには、このコマンドの **no** 形式を使用します。

ethernet uni {bundle [all-to-one] | multiplex}

no ethernet uni {bundle | multiplex}

構文の説明

bundle	多重化しないでバンドルをサポートするように UNI を設定します。このサービスでは、UNI において、1 つまたは複数のカスタマー エッジ (CE) VLAN ID がマッピングされた 1 つのイーサネット仮想接続 (EVC) のみがサポートされます。
all-to-one	(任意) UNI において、すべての CE VLAN がマッピングされた 1 つの EVC によるバンドルをサポートするように UNI を設定します。
multiplex	バンドルしないで多重化をサポートするように UNI を設定します。UNI には、それぞれに 1 つの CE VLAN ID がマッピングされた 1 つ以上の EVC を設定できます。

デフォルト

バンドルまたは多重化属性が設定されていない場合、デフォルトは多重化を使用したバンドリングです。その場合、UNI には、それぞれに 1 つ以上の CE VLAN VLAN がマッピングされた 1 つ以上の EVC を設定できます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

UNI 属性によって、VLAN のバンドル、EVC の多重化、およびこれらの組み合わせについてのインターフェイスの機能が決定されます。

UNI にバンドルと多重化両方のサービスを行わせたい場合、バンドルまたは多重化を設定する必要はありません。バンドルまたは多重化だけする場合、これを適切に設定する必要があります。

UNI サービス タイプを設定、変更、削除する場合、EVC および CE-VLAN ID 設定をチェックして、コンフィギュレーションと UNI サービス タイプが一致していることを確認します。設定が一致しない場合、コマンドは拒否されます。

ethernet lmi ce-vlan map any サービス コンフィギュレーション コマンドを使用する場合、事前に **all-to-one** バンドルをインターフェイスで設定する必要があります。詳細については、[ethernet lmi ce-vlan map](#) の項を参照してください。

例 次に、多重化しないでバンドルを設定する例を示します。

```
Switch(config-if)# ethernet uni bundle
```

UNI サービス タイプを確認するには、**show ethernet service interface 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
show ethernet service interface	サービス タイプなど、インターフェイスのイーサネット サービス インスタンスに関する情報を表示します。

ethernet uni id

ユーザ ネットワーク インターフェイス (UNI) ID を作成するには、**ethernet uni** 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。UNI ID を削除するには、このコマンドの **no** 形式を使用します。

ethernet uni id name

no ethernet uni id

構文の説明

<i>name</i>	イーサネット UNI ID を識別します。同じサービス インスタンスに属するすべての UNI の名前はそれぞれ、一意である必要があります。名前の長さは 64 文字までです。
-------------	--

デフォルト

UNI ID は作成されません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポートに UNI ID を設定すると、その ID はポートに設定されたすべてのメンテナンス エンド ポイント (MEP) のデフォルトの名前として使用されます。

カスタマー エッジ (CE) デバイスに直接接続されているすべてのポートで **ethernet uni id name** コマンドを入力する必要があります。指定された ID がデバイス上で一意でない場合は、エラー メッセージが表示されます。

例

次に、一意の UNI を識別する方法を示します。

```
Switch(config-if)# ethernet uni id test2
```

関連コマンド

コマンド	説明
show ethernet service interface	サービス タイプなど、インターフェイスのイーサネット サービス インスタンスに関する情報を表示します。

exceed-action

認定情報レート（CIR）または最大情報レート（PIR）の適合レートと、適合レートに超過バーストを加えたレートの間レートのパケットに対するポリシーマップクラスに複数のアクションを設定するには、**exceed-action** ポリシーマップクラス ポリシング コンフィギュレーション コマンドを使用します。アクションをキャンセルしたり、デフォルトアクション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。

```
exceed-action {drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit}}
```

```
no exceed-action {drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit}}
```

構文の説明

drop	パケットをドロップします。
set-cos-transmit <i>new-cos-value</i>	パケットの新しいサービス クラス（CoS）値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 CoS 値に指定できる範囲は 0 ～ 7 です。
set-dscp-transmit <i>new-dscp-value</i>	パケットの新しい DiffServ コード ポイント（DSCP）値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 DSCP 値に指定できる範囲は 0 ～ 63 です。
set-prec-transmit <i>new-precedence-value</i>	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 IP precedence 値に指定できる範囲は 0 ～ 7 です。
set-qos-transmit <i>qos-group-value</i>	パケットの新しい Quality of Service（QoS）グループ値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 QoS 値に指定できる範囲は 0 ～ 99 です。
cos	(任意) 着信パケットの CoS 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
dscp	(任意) 着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
precedence	(任意) 着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
table <i>table-map name</i>	(任意) 上記の <i>from-type</i> キーワードとともに使用します。拡張パケットマーキングに使用するテーブル マップを指定します。このテーブル マップを使用して、アクションの <i>from-type</i> パラメータに基づき、アクションの <i>to-type</i> がマーキングされます。
transmit	(任意) パケットを変更せずに送信します。

デフォルト

デフォルトのアクションは、パケットのドロップです。

コマンドモード ポリシーマップ クラス ポリシング設定

コマンド履歴	リリース	変更箇所
	12.2(53)EX	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 レートが、設定された適合レートと、適合レートに超過バーストを加えたレートの間である場合の packets に対する超過アクションを設定します。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。

超過アクションは、パケットの変更なしでの送信、明示値を使用したマーキング、および拡張パケットマーキングのすべての組み合わせの使用に設定できます。拡張パケットマーキングによって、任意の着信 QoS マーキングおよびテーブル マップに基づいて QoS マーキングを変更できます。スイッチでは、同じクラスに複数の QoS パラメータをマーキングし、同時に conform-action、exceed-action、violate-action マーキングを行う機能もサポートされています。

ポリシーマップ クラス ポリシング コンフィギュレーション モードにアクセスするには、**police** ポリシーマップ クラス コマンドを入力します。詳細については、**police** コマンドを参照してください。

このコマンドを使用して、トラフィック クラスに対して 1 つ以上の超過アクションを設定できます。

例 次に、情報レートを 23000 ビット/秒に、バースト レートを 10000 ビット/秒に設定するポリシー マップで複数のアクションを設定する例を示します。

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 23000 10000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-prec-transmit prec table
policed-prec-table-map-name
Switch(config-pmap-c-police)# 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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
	conform-action	CIR に適合するトラフィックに対して実行するアクションを定義します。
	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。
	violate-action	適合レートに超過バーストを加えたレートよりも大きいレートのトラフィックで実行されるアクションを定義します。

fcs-threshold

フレーム チェック シーケンス (FCS) ビットエラー レートを設定するには、**fcs-threshold** 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場合は、このコマンドの **no** 形式を使用します。

fcs-threshold value

no fcs-threshold value

構文の説明

value 値範囲は 6 ~ 11 で、 10^{-6} ~ 10^{-11} ビットエラー レートを示します。

デフォルト

デフォルトは 8 です。これは、イーサネット標準の 10^{-8} ビットエラー レートを示します。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

イーサネット標準の上限ビットエラー レートは 10^{-8} です。CGS 2520 スイッチで設定可能なビットエラー レートの範囲は 10^{-6} ~ 10^{-11} です。スイッチのビットエラー レートは自然数です。ビットエラー レートに 10^{-9} を設定する場合は、係数に 9 を入力します。

スイッチに FCS エラー ヒステリシスしきい値を設定して、実際のビットエラー レートの変動が設定したビットエラー レートに接近した場合のアラームを防止するには、**alarm facility fcs hysteresis** 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、ポートの FCS ビットエラー レートを 10^{-10} に設定する方法を示します。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# fcs-threshold 10
```

関連コマンド

コマンド	説明
alarm facility fcs-hysteresis	スイッチの FCS ヒステリシスしきい値をポートに設定された FCS ビットエラー レートの許容変動率で設定します。
show fcs-threshold	インターフェイスそれぞれの FCS エラー ビット レート設定を正数の係数として表示します。

flowcontrol

インターフェイスの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)

Cisco CGS 2520 スイッチはポーズ フレームのみを受信できます。

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働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働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	変更箇所
12.2(53)EX	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。ポートがユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) の場合、**flowcontrol** コマンドを使用する前に **no shutdown** インターフェイス コンフィギュレーション コマンドを使用してインターフェイスをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノードインターフェイス (NNI) はデフォルトでイネーブルです。

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。ポートでは、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 2-3 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 2-3 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 gigabitethernet0/1
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。

hw-module module logging onboard

オンボード障害ロギング (OBFL) をイネーブルにするには、**hw-module module logging onboard** 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。

hw-module module [*slot-number*] **logging onboard** [*message level level*]

no hw-module module [*slot-number*] **logging onboard** [*message level*]

構文の説明

<i>slot-number</i>	(任意) スロット番号は常に 1 で、CGS 2520 には関連しません。
<i>message level level</i>	(任意) フラッシュ メモリに保存されるハードウェア関連のメッセージの重大度を指定します。指定できる範囲は 1 ~ 7 です。1 が最も高い重大度です。

デフォルト

OBFL はイネーブルになっており、すべてのメッセージが表示されます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

OBFL はイネーブルにしておき、フラッシュ メモリに保存されたデータは消さないようにすることを推奨します。

OBFL データ ログ内のタイム スタンプを正確にするには、システム クロックを手動で設定するか、またはネットワーク タイム プロトコル (NTP) を使用して設定します。

message level level パラメータを入力しなければ、ハードウェア関連のすべてのメッセージがスイッチによって生成され、フラッシュ メモリに保存されます。

任意のスロット番号は常に 1 です。**hw-module module** [*slot-number*] **logging onboard** [*message level level*] コマンドを入力することは、**hw-module module logging onboard** [*message level level*] コマンドを入力することと同じです。

例

次に、スイッチ上で OBFL をイネーブルにし、ハードウェア関連のメッセージがフラッシュ メモリに保存されるように指定する例を示します。

```
Switch(config)# hw-module module logging onboard
```

次に、スイッチ上で OBFL をイネーブルにし、重大度 1 のハードウェア関連のメッセージだけがフラッシュ メモリに保存されるように指定する例を示します。

```
Switch(config)# hw-module module logging onboard message level 1
```

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

■ hw-module module logging onboard

関連コマンド

コマンド	説明
clear logging onboard	フラッシュメモリ内の OBFL データを削除します。
show logging onboard	OBFL 情報を表示します。

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	変更箇所
12.2(53)EX	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 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。

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。



(注) CDP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

interface port-channel

- 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、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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

interface range

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、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	変更箇所
12.2(53)EX	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コンフィギュレーション 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 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)

interface range

- **gigabitethernet** module/{first port} - {last port} (module は常に 0)
物理インターフェイス
 - モジュールは常に 0 です。
 - 指定できる範囲は、type 0/number - number です (例: **gigabitethernet0/1 - 2**)。
- **port-channel** port-channel-number - port-channel-number (port-channel-number は 1 ~ 48)



(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 gigabitethernet0/1 -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 fastethernet0/1 - 2, gigabitethernet0/1 - 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。

port-range では単一のインターフェイスも指定できます (この場合、**interface interface-id** グローバル コンフィギュレーション コマンドと同様)。



(注)

インターフェイス範囲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 gigabitethernet0/1 - 2
Switch(config-if-range)#
```

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 gigabitethernet0/1 - 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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

interface vlan

スイッチ仮想インターフェイス (SVI) 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	変更箇所
12.2(53)EX	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、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復元しますが、以前の設定の大半は失われます。

スイッチ上で設定された 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もあります。**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。詳細については、**sdm prefer** コマンドを参照してください。

例

次に、VLAN ID 23 を作成し、インターフェイス コンフィギュレーション モードを開始する例を示します。

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

■ interface vlan

設定を確認するには、**show interfaces** および **show interfaces 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 interfaces vlan <i>vlan-id</i>	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。スイッチでメトロ IP アクセス イメージが稼動している場合、レイヤ 3 インターフェイスへのアクセスを制御することもできます。

```
ip access-group {access-list-number | name} {in | out}
```

```
no ip access-group [access-list-number | name] {in | out}
```

構文の説明

<i>access-list-number</i>	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。
<i>name</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

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。

スイッチでは、レイヤ 3 をサポートするため、メトロ IP アクセス イメージが稼動している必要があります。

レイヤ 2 インターフェイス (ポート ACL) またはレイヤ 3 インターフェイスにアクセス リストを適用するためにこのコマンドを使用できます。ただし、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 は受信方向に対してだけ適用できます。**out** キーワードはレイヤ 2 のインターフェイスでサポートされていません。
- 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。
- ポート ACL はロギングをサポートしていないため、IP ACL で **log** キーワードを指定しても無視されます。

- 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 ACL が常に優先されます。入力ポートの ACL と VLAN マップが両方適用されている場合、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。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; インターネット制御メッセージプロトコル)** 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 gigabitethernet0/1
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。構文情報については、『 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 』> 「 IP Services Commands 」を選択してください。
ip access-list	名前付き ACL を設定します。構文情報については、『 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 』> 「 IP Services Commands 」を選択してください。
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。構文情報については、『 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 』> 「 IP Services Commands 」を選択してください。
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。構文情報については、『 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 』> 「 IP Services Commands 」を選択してください。

ip address

レイヤ 2 スイッチの IP アドレスを設定したり、レイヤ 3 スイッチの各スイッチ仮想インターフェイス (SVI) またはルーテッドポートの IP アドレスを設定したりするには、**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**]



(注)

スイッチでメトロ IP アクセス イメージが稼動している場合にだけルーテッドポートおよび SVI を設定できます。

構文の説明

<i>ip-address</i>	IP アドレス。
<i>subnet-mask</i>	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	変更箇所
12.2(53)EX	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; インターネット制御メッセージプロトコル) 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 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。詳細については、**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witch 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、スイッチ上のレイヤ 3 ポートに IP アドレスを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス 一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

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

<i>arp-acl-name</i>	ARP Access Control List (ACL; アクセス コントロール リスト) の名前
<i>vlan-range</i>	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 内にあることを意味し、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	変更箇所
12.2(53)EX	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 ip arp inspection vlan <i>vlan-range</i>	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タスを表示します。

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	変更箇所
12.2(53)EX	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** 回復機能により、回復設定に従ってポートが **errdisable** ステートから自動的に解除されます。

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間隔を 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 ip arp inspection 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せん。

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	変更箇所
12.2(53)EX	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。

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 メッセージを每秒生成します。

```
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 Access Control List (ACL; アクセス コントロール リスト) 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 ip arp inspection 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	変更箇所
12.2(53)EX	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 gigabitethernet0/1
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 ip arp inspection 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 ip arp inspection 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	変更箇所
12.2(53)EX	このコマン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、別のコマンドが 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。

■ ip arp inspection validate

- 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 ip arp inspection 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タスを表示します。

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

<i>vlan-range</i>	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	変更箇所
12.2(53)EX	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 Access Control List (ACL; アクセス コントロール リスト) を定義します。
show ip arp inspection vlan <i>vlan-range</i>	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タスを表示します。

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

<i>vlan-range</i>	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。 <ul style="list-style-type: none"> • matchlog : Access Control Entry (ACE; アクセス コントロール エントリ) 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。 <ul style="list-style-type: none"> • 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	変更箇所
12.2(53)EX	このコマン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 ip arp inspection 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 ip arp inspection 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タスを表示します。

ip device tracking maximum

レイヤ 2 ポートで IP ポートセキュリティ バインディングのトラッキングをイネーブルにするには、**ip device tracking maximum** コマンドを使用します。信頼できないレイヤ 2 インターフェイスで IP ポートセキュリティをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip device tracking maximum {number}

no ip device tracking maximum {number}

構文の説明

number ポートの IP デバイス トラッキング テーブルに作成するバインディングの数を指定します。有効値の範囲は 0 ~ 2048 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

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

例

次の例では、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用して IP ポートセキュリティを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)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

設定を確認するには、**show ip verify source** 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	信頼できないレイヤ 2 インターフェイスで IP ソース ガードをイネーブルにします。
show ip verify source	特定のインターフェイス上の IP ソース ガード設定とフィルタを表示します。

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	変更箇所
12.2(53)EX	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** 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	VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
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 ~ 4904 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	変更箇所
12.2(53)EX	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。

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。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  
gigabitethernet0/1 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:/filename | ftp://user:password@host/filename |
http://[[username:password]@]{hostname | host-ip}[/directory]/image-name.tar |
rctp://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:/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。
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。
rctp://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; リモート コピー プロトコル) 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	DHCP スヌーピングのバインディング データベースが変更されたあとのデータベース転送プロセスを停止する時間 (秒単位) 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。無期限を定義するには 0 を使用します。
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	変更箇所
12.2(53)EX	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せん。

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 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初めて書き込む前に、この URL に空のファイルを作成しておく必要があります。

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
```

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 データ挿入はイネーブルです。

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	変更箇所
12.2(53)EX	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** 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 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 allowed-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 allowed-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。スイッチがエッジスイッチからのこれらのパケットをドロップするよう設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-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	変更箇所
12.2(53)EX	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 allowed-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せん。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)

ip dhcp snooping information option allowed-untrusted コマンドを、信頼できないデバイスが接続されている集約スイッチに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 allowed-untrusted
```

設定を確認するには、**show ip dhcp 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
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 <i>ASCII-string</i>	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witch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	変更箇所
	12.2(53)EX	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

<i>rate</i>	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	変更箇所
12.2(53)EX	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、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** 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	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

DHCP スヌーピングを実行するためにポートを信頼できるポート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	変更箇所
12.2(53)EX	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** 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 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 mac-address

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スイッチを設定するには、スイッチ スタックまたはスタンドアロンスイッチ上で **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	変更箇所
12.2(53)EX	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** 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 snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping vlan

DHCP スヌーピングを VLAN 上で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。DHCP スヌーピングを 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。

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

構文の説明

vlan *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	変更箇所
12.2(53)EX	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** 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 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* information option format-type circuit-id [override] string *ASCII-string*

no ip dhcp snooping vlan *vlan* information option format-type circuit-id [override] string

構文の説明

vlan <i>vlan</i>	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 <i>ASCII-string</i>	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	変更箇所
12.2(53)EX	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 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せられた場合、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
```

■ ip dhcp snooping vlan information option format-type circuit-id string

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) **show ip dhcp snooping** ユーザ EXEC コマンドでは、リモート ID 設定を含むグローバル コマンド出力だけが表示されます。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インターネット グループ管理プロトコル (IGMP) 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 グループに参加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	<i>profile number</i> 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	変更箇所
	12.2(53)EX	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 物理インターフェイスにだけ IGMP フィルタを適用できます。 ルーテッド ポート、スイッチ仮想インターフェイス (SVI)、または EtherChannel グループに属するポートに対しては IGMP フィルタを適用できません。 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。 <pre>Switch(config)# interface gigabitethernet0/2 Switch(config-if)# ip igmp filter 22</pre> 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。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。

ip igmp max-groups

レイヤ 2 インターフェイスが加入可能なインターネット グループ管理プロトコル (IGMP) 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、**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

<i>number</i>	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 ICMP 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	変更箇所
12.2(53)EX	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、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。

ip igmp max-groups

- 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

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

```
Switch(config)# interface gigabitethernet0/2
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 gigabitethernet0/1
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。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。

ip igmp profile

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	変更箇所
12.2(53)EX	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に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
```

■ ip igmp profile

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 <i>vlan-id</i>	(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	変更箇所
12.2(53)EX	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。

■ ip igmp snooping

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 detail	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	
vlan <i>vlan-id</i>	(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。
<i>time</i>	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	変更箇所
	12.2(53)EX	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、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 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。

■ ip igmp snooping last-member-query-interval

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 <i>vlan-id</i>	(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 <i>ip-address</i>	(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 <i>response-time</i>	(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 <i>interval-count</i>	(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 <i>count</i> interval <i>interval</i>]	(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。 <ul style="list-style-type: none"> count <i>count</i> : 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 <i>interval</i> : 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 <i>version</i>	(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	変更箇所
12.2(53)EX	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に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せん。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	変更箇所
12.2(53)EX	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、1 つのマルチキャスト 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。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。

■ ip igmp snooping report-suppression

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; トポロジ変更通知) 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 <i>count</i>	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	変更箇所
12.2(53)EX	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により、トポロジの変更によって発生する可能性のあるマルチキャスト トラフィックの損失を防ぐことができます。**ip igmp snooping tcn flood query count** コマンドを使用して TCN フラッディングクエリー数を 1 に設定した場合、フラッディングは一般クエリーを 1 つ受信した時点で停止します。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続きます。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。

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ドリングを 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; トポロジ変更通知) 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ド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。

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ドリングは、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	変更箇所
12.2(53)EX	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ドリングします。異なるマルチキャストグループのホストに接続しているポートが複数ある場合、フラッドリングトラフィックがリンクの容量を超え、パケット損失が発生する場合があります。このフラッドリング動作は適切でない可能性があります。

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、フラッドリ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ドリングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
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) スヌーピング即時脱退処理をイネーブルにするには、**ip igmp snooping vlan *vlan-id* 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

<i>vlan-id</i>	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	変更箇所
12.2(53)EX	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 の各ポート上で最大 1 つのレシーバ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 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 detail	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 vlan *vlan-id* 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 pim-dvmrp}

no ip igmp snooping vlan *vlan-id* mrouter {interface *interface-id* | learn pim-dvmrp}

構文の説明

<i>vlan-id</i>	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 <i>interface-id</i>	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。有効なインターフェイスは、物理インターフェイスおよびポート チャネルです。ポート チャネル範囲は 1 ~ 48 です。
learn pim-dvmrp	マルチキャスト ルータの学習方式を指定します。Cisco CGS 2520 スイッチでサポートされている学習方式は、IGMP クエリーおよびプロトコル独立型マルチキャスト ディスタンス ベクトル マルチキャスト ルーティング プロトコル (PIM-DVMRP) パケットのスヌーピングによってマルチキャスト ルータ ポートを学習するようにスイッチを設定する pim-dvmrp です。

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	変更箇所
12.2(53)EX	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 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 gigabitethernet0/2
```

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。

■ ip igmp snooping vlan mrouter

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 detail	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

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 vlan *vlan-id* 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

<i>vlan-id</i>	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。
<i>ip-address</i>	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 <i>interface-id</i>	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。 <ul style="list-style-type: none"> • fastethernet <i>interface number</i> : ファストイーサネット IEEE 802.3 インターフェイス • gigabitethernet <i>interface number</i> : ギガビットイーサネット IEEE 802.3z インターフェイス • port-channel <i>interface number</i> : 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	変更箇所
12.2(53)EX	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 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 mrouter interface gigabitethernet0/2
```

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。

■ ip igmp snooping vlan static

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 detail	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 sla responder twamp

Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) レスポンダとしてスイッチを設定するには、**ip sla responder twamp** 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 SLA TWAMP レスポンダ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 sla responder twamp [timeout seconds]

no ip sla responder twamp [timeout seconds]

構文の説明

timeout seconds (任意) このセッションが非アクティブになってから TWAMP セッションを終了するまでの秒数を指定します。指定できる範囲は 1 ~ 604800 秒です。デフォルトは、900 秒です。

デフォルト

IP SLA TWAMP レスポンダ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	変更箇所
12.2(53)EX	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 sla responder twamp コマンドを入力すると、IP SLA TWAMP リフレクタ 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。

- **default** : コマンドをそのデフォルトに設定します。
- **exit** : IP SLA TWAMP リフレクタ 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。
- **timeout seconds** : セッションが非アクティブの場合に終了されるまでの最大時間を指定します。指定できる範囲は 1 ~ 604800 秒です。デフォルトは、900 秒です。

TWAMP サーバとリフレクタが機能するには、TWAMP 制御デバイスも設定する必要があります。制御デバイスはクライアントおよびセッション送信元として機能します。これらの機能は、シスコ デバイスでは設定されません。

例

次に、スイッチを IP SLA TWAMP レスポンダとして設定する例を示します。

```
Switch(config)# ip sla responder twamp
Switch(config-twamp-ref)# timeout inactivity 900
```

■ ip sla responder twamp

関連コマンド

コマンド	説明
ip sla responder	一般的な IP SLA 運用に対して Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) レスポンダをイネーブルにします。
ip sla server twamp	双方向アクティブ測定プロトコル (TWAMP) サーバとしてスイッチを設定します。
show ip sla standards	(任意) スイッチに設定されている IP SLA 標準を表示します。
show ip sla twamp connection {detail requests}	(任意) 現在の Cisco IOS IP Service Level Agreements (SLA; サービス レベル契約) の Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) 接続を表示します。

ip sla server twamp

双方向アクティブ測定プロトコル (TWAMP) サーバとしてスイッチを設定するには、**ip sla server twamp** 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 SLA TWAMP サーバ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 sla server twamp

no ip sla server twamp

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

IP SLA TWAMP サーバ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	変更箇所
12.2(53)EX	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 sla server twamp コマンドを入力すると、IP SLA TWAMP サーバ 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。

- **default** : コマンドをそのデフォルトに設定します。
- **exit** : IP SLA TWAMP サーバ 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。
- **port port-number** : TWAMP 制御トラフィックの送信元ポートを指定します。有効なポート番号は 1 ~ 65535 です。
- **timer inactivity seconds** : セッションが非アクティブの場合に終了されるまでの最大時間を指定します。指定できる範囲は 1 ~ 6000 秒です。デフォルト値は 900 秒です。

TWAMP サーバとリフレクタが機能するには、TWAMP 制御デバイスも設定する必要があります。制御デバイスはクライアントおよびセッション送信元として機能します。これらの機能は、シスコ デバイスでは設定されません。

例

次に、スイッチを IP SLA TWAMP サーバとして設定する例を示します。

```
Switch(config)# ip sla server twamp
Switch(config-twamp-srvr)# port 862
Switch(config-twamp-srvr)# timer inactivity 540
```

関連コマンド

コマンド	説明
ip sla responder	一般的な IP SLA 運用に対して Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) レスポンダをイネーブルにします。
ip sla responder twamp	Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) レスポンダとしてスイッチを設定します。
show ip sla standards	(任意) スイッチに設定されている IP SLA 標準を表示します。
show ip sla twamp connection {detail requests}	(任意) 現在の Cisco IOS IP Service Level Agreements (SLA; サービス レベル契約) の Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) 接続を表示します。

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 <i>vlan-id</i>	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 <i>interface-id</i>	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	変更箇所
12.2(53)EX	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
gigabitethernet0/1
```

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
gigabitethernet0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet0/1
```

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。

■ ip source binding

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。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]

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。

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	変更箇所
12.2(53)EX	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。構文情報については、「Cisco IOS Release 12.2 Configuration Guides and Command References」> 『Cisco IOS Security Command Reference, Release 12.2』> 「Other Security Features」> 「Secure Shell Commands」を選択してください。
show ssh	SSH サーバのステータスを表示します。構文情報については、「Cisco IOS Release 12.2 Configuration Guides and Command References」> 『Cisco IOS Security Command Reference, Release 12.2』> 「Other Security Features」> 「Secure Shell Commands」を選択してください。

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	変更箇所
12.2(53)EX	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。

■ 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 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。構文情報については、『Cisco IOS IP Addressing Services Command Reference, Release 12.4』> 「ARP Commands」を参照してください。
show arp	ARP テーブル内のエントリを表示します。構文情報については、『Cisco IOS IP Addressing Services Command Reference, Release 12.4』> 「ARP Commands」を参照してください。

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	変更箇所
12.2(53)EX	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。

ip sticky-arp (インターフェイス コンフィギュレーション)

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。構文情報については、『Cisco IOS IP Addressing Services Command Reference, Release 12.4』> 「ARP Commands」を参照してください。
show arp	ARP テーブル内のエントリを表示します。構文情報については、『Cisco IOS IP Addressing Services Command Reference, Release 12.4』> 「ARP Commands」を参照してください。

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 {vlan dhcp-snooping | tracking} [port-security]

no ip verify source {vlan dhcp-snooping | tracking} [port-security]

構文の説明

vlan dhcp-snooping	信頼できないレイヤ 2 DHCP スヌーピング インターフェイスで IP ソース ガードをイネーブルにします。
tracking	ポートで固定 IP アドレス ラーニングを学習するために IP ポート セキュリティをイネーブルにします。
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 の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	変更箇所
12.2(53)EX	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、ポート単位で VLAN 10 ~ 20 で IP ソース ガードを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)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
```

```

Switch(config)# interface gigabitEthernet0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip verify source interface gigabitEthernet0/1
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----  -
Gi0/1     ip-mac       active       10.0.0.1        -----
Gi0/1     ip-mac       active       deny-all        -----
Switch#

```

次の例では、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用して IP ポート セキュリティを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)# ip device tracking
Switch(config)# interface gigabitEthernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

```

設定を確認するには、**show ip verify source** 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 device tracking maximum	レイヤ 2 ポートで IP ポート セキュリティ バインディングのトラッキングをイネーブルにします。
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping limit rate	インターフェイスが 1 秒間に受信できる DHCP メッセージの数を設定します。
ip dhcp snooping information option	DHCP オプション 82 データ挿入をイネーブルにします。
ip dhcp snooping trust	信頼できる VLAN で DHCP スヌーピングをイネーブルにします。
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 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 エントリを表示します。
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。

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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

構文の説明

<i>access-list-name</i>	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	変更箇所
12.2(53)EX	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 | routing | 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。

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。

IPv6 ACL 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、**deny (IPv6 アクセスリスト コンフィギュレーション)** 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。

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 ネイバー探索を許可します。ICMPv6 ネイバー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 ネイバー探索プロセスでは、IPv6 ネットワーク層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 ネイバー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 ネイバー探索プロセスと同等の Address Resolution Protocol (ARP) は、別のデータリンク層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 Switch Virtual Interface (SVI; 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 gigabitethernet0/3
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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

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	変更箇所
12.2(53)EX	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 | routing | 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。

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 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

次に、IPv6 アドレスを取得して、**rapid-commit** オプションをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/1
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

DHCP for IPv6 (DHCPv6) サーバからオプションを要求するよう 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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

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

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	変更箇所
12.2(53)EX	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 | routing | 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。

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 から取得するときだけにこのコマンドを確認します。インターフェイスが IPv6 アドレスを取得したあと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 gigabitethernet0/1
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 動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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できます。

構文の説明

<i>number</i>	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	変更箇所
12.2(53)EX	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。

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 の応答がない場合はアドレスが使用されていないことを示すため、サーバは要求元クライアントにそのアドレスを割り当てます。

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
<code>clear ipv6 dhcp conflict</code>	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。
<code>show ipv6 dhcp conflict</code>	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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

構文の説明

<i>poolname</i>	DHCPv6 プールのユーザ定義名。プール名には象徴的な文字列 (<i>Engineering</i> 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	変更箇所
12.2(53)EX	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。

DHCPv6 プール コンフィギュレーション モードのコマンドは次のようになります。

- **address prefix IPv6-prefix** : アドレス割り当てのアドレス プレフィックスを設定します。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 プレフィックスを設定します。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 プレフィッ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** : 次のコンフィギュレーション コマンドを使用して、DHCPv6 ベンダー固有のコンフィギュレーション モードをイネーブルにします。
 - **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、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とおりに入力します。

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 アドレスを照合できます。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
<code>ipv6 dhcp server</code>	インターフェイスで DHCPv6 サービスをイネーブルにします。
<code>show ipv6 dhcp pool</code>	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**] [**allow-hint**] [**rapid-commit**] [**preference value**]

no ipv6 dhcp server



(注)

このコマンドは、メトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できます。

構文の説明

<i>poolname</i>	(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 (<i>Engineering</i> 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。
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。
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。有効な範囲は 0 ~ 255 です。デフォルト値は 0 です。
rapid-commit	(任意) 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	変更箇所
12.2(53)EX	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 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 キーワードを入力すると、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が自動的に決定されます。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。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。

allow-hint のキーワードを入力した場合、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。

preference キーワードを 0 以外の値に設定すると、サーバはアドバタイズ メッセージにプリファレンス オプションを追加して、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。

rapid-commit キーワードを入力すると、2 つのメッセージ交換を使用できます。

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。スイッチまたは VLAN 上で MLD スヌーピ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。

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 IP Services イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できます。

構文の説明

vlan <i>vlan-id</i>	(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	変更箇所
12.2(53)EX	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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

構文の説明

vlan <i>vlan-id</i>	(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。
<i>integer_value</i>	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	変更箇所
12.2(53)EX	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回答できます (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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できます。

構文の説明

vlan <i>vlan-id</i>	(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。
<i>integer_value</i>	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	変更箇所
12.2(53)EX	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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できます。

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	変更箇所
12.2(53)EX	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。

コマンド	説明
<code>sdm prefer</code>	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。
<code>show ipv6 mld snooping</code>	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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できます。

構文の説明

vlan <i>vlan-id</i>	(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。
<i>integer_value</i>	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	変更箇所
12.2(53)EX	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; トポロジ変更通知) 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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

構文の説明

flood query count <i>integer_value</i>	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	変更箇所
12.2(53)EX	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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

構文の説明

vlan <i>vlan-id</i>	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 <i>ipv6-multicast-address</i>	(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 <i>interface-id</i>	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	変更箇所
12.2(53)EX	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 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、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。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 {in | out}
```



(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

<i>access-list-name</i>	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。 out キーワードは、スイッチでメトロ IP アクセス イメージが稼動している場合にだけ、レイヤ 3 インターフェイスでサポートされます。

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	変更箇所
12.2(53)EX	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 | routing | 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。

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せん。

スイッチでメトロ IP アクセス イメージが稼動している場合、ACL をレイヤ 3 インターフェイスの発信または着信トラフィック (ルータ ACL)、あるいはレイヤ 2 インターフェイスの着信トラフィック (ポート ACL) に適用することができます。スイッチでメトロ アクセス イメージが稼動している場合、ACL をレイヤ 2 インターフェイスの着信管理トラフィックだけに適用することができます。これらのイメージは、ルータ ACL をサポートしません。

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 が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 gigabitethernet0/1
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。

I2protocol-tunnel

アクセスポート、トランクポート、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、**I2protocol-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; VLAN トランッキングプロトコル) 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; ポート集約プロトコル)、Link Aggregation Control Protocol (LACP)、または UniDirectional Link Detection (UDLD; 単方向リンク検出) 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。

```
I2protocol-tunnel [cdp | stp | vtp] [drop-threshold [cdp | stp | vtp | point-to-point [pagp | lacp | udld]] value] [point-to-point [pagp | lacp | udld]] [shutdown-threshold [cdp | stp | vtp | point-to-point [pagp | lacp | udld]] value]
```

```
no I2protocol-tunnel [cdp | stp | vtp] [drop-threshold [cdp | stp | vtp | point-to-point [pagp | lacp | udld]]] [point-to-point [pagp | lacp | udld]] [shutdown-threshold [cdp | stp | vtp | point-to-point [pagp | lacp | udld]]]
```

構文の説明

I2protocol-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。
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。
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。
<i>value</i>	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	変更箇所
12.2(53)EX	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。

**(注)**

スイッチは VTP をサポートしません。CDP および STP は、ネットワーク ノード インターフェイス (NNI) 上ではデフォルトでイネーブルになっています。拡張ネットワーク インターフェイス (ENI) 上ではデフォルトでディセーブルになっていますが、イネーブルにできます。ユーザ ネットワーク インターフェイス (UNI) は、これらのプロトコルをサポートしません。

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。

**(注)**

NNI および ENI だけが PAgP および LACP をサポートします。

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 に保存されます。



(注)

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
<code>l2protocol-tunnel cos</code>	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。
<code>show errdisable recovery</code>	errdisable の回復タイマー情報を表示します。
<code>show l2protocol-tunnel</code>	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、サービス クラス (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

<i>value</i>	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	変更箇所
12.2(53)EX	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 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



(注) LACP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

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	変更箇所
12.2(53)EX	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。このコマンドは、LACP が設定済みの EtherChannel ポートにのみ有効です。インターフェイスがユーザ ネットワーク インターフェイス (UNI) の場合 **lacp port-priority** を設定する前に NNI または ENI にインターフェイスを変更する、**port-type nni** または **port-type eni** 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。ハードウェアの制限により互換性のあるすべてのポートをアクティブにできない場合は、プライオリティを使用して、スタンバイ モードにする必要があるポートを決定します。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。

■ lacp port-priority

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 gigabitethernet0/1
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	すべてのチャンネル グループまたは指定のチャンネル 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



(注)

LACP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

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	変更箇所
12.2(53)EX	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。これはグローバル コンフィギュレーション コマンドですが、プライオリティは LACP にすでに設定されている物理ポートがある EtherChannel でのみ有効です。

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、チャン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 プライオリティのシステム値の数値が小さいスイッチ (より高いプライオリティ値) が制御スイッチになります。いずれのスイッチも同じ LACP システム プライオリティである場合 (たとえば、いずれ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 モードのポート (ポートステート フラグが H になっています) を確認するには、**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。

■ lACP system-priority

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ー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

<i>number</i>	(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 ~ 2 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	変更箇所
12.2(53)EX	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ポート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が使用されます。

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スイッチポート、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。個々のダウンストリームインターフェイスは、1 つ以上のアップストリームインターフェイスに関連付けることができます。アップストリームインターフェイス同士はバンドルでき、各ダウンストリームインターフェイスは、複数のアップストリームインターフェイスで構成されたリンクステートグループと呼ばれる単一グループに関連付けることができます。

ダウンストリームインターフェイスのリンクステートは、関連付けられているリンクステートグループのアップストリームインターフェイスのリンクステートに依存します。リンクステートグループ内のすべてのアップストリームインターフェイスがリンクダウンステートにある場合、関連付けられたダウンストリームインターフェイスは強制的にリンクダウンステートになります。リンクステートグループ内のアップストリームインターフェイスのいずれか 1 つがリンクアップステートである場合、関連付けられたダウンストリームインターフェイスは、リンクアップステートに移行するか、またはリンクアップステートを維持することができます。

link state group

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 1 つにつき、設定できるリンクステート グループは 2 つだけです。

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 gigabitethernet0/11 - 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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

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 ~ 2 です。デフォルトは 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	変更箇所
12.2(53)EX	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 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。
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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_comm_and_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

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	Emergency Location Information (ELIN; 緊急ロケーション情報) 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	変更箇所
12.2(53)EX	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。
<i>word</i>	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。
<i>id</i>	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	変更箇所
12.2(53)EX	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)# int g1/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

```
Switch(config-if)# int g2/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

設定を確認するには、**show location civic interface** 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)# int g2/0/2
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 ログ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	変更箇所
12.2(53)EX	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 ログ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 ステータス 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。ただし、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

power-inline-status PoE メッセージのロギングをイネーブルにします。

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	変更箇所
12.2(53)EX	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-inline-status キーワードは、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* [*min-file-size*]] [*severity-level-number* | *type*]

no logging file *filesystem:filename* [*severity-level-number* | *type*]

構文の説明

<i>filesystem:filename</i>	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。 ローカル フラッシュ ファイル システムの構文： flash:
<i>max-file-size</i>	(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。
<i>min-file-size</i>	(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。
<i>severity-level-number</i>	(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 <i>type</i> オプションを参照してください。
<i>type</i>	(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。 <ul style="list-style-type: none"> • 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) • information : 情報メッセージ (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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ログファイルはスイッチの内部バッファに ASCII テキスト形式で保存されます。ロギングされたシステムメッセージにアクセスするには、スイッチの **Command-Line Interface (CLI; コマンドラインインターフェイス)** を使用するか、または適切に設定された **Syslog** サーバにこれらのシステムメッセージを保存します。スイッチに障害が生じた場合は、それ以前に **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ログを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値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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

mac access-group

MAC アクセス コントロール リスト (ACL) 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

<i>name</i>	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	変更箇所
12.2(53)EX	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。



(注) MAC 拡張 ACL を設定する方法の詳細については、このリリースに対するソフトウェア 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 gigabitethernet0/1
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 mac access-group	スイッチで設定される MAC ACL を表示します。
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 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

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。



(注)

レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

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	変更箇所
12.2(53)EX	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。

VLAN マップまたはレイヤ 2 インターフェイスに、名前付き MAC 拡張 ACL を適用できます。

レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

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 \(MAC アクセス リスト コンフィギュレーション\)](#) 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。詳細については、[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。



(注)

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)	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)。
permit (MAC アクセス リスト コンフィギュレーション)	
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	変更箇所
12.2(53)EX	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ディングが起これにくくなります。

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 ラーニング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 ラーニング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

デフォルト

デフォルトでは、MAC アドレス ラーニングはすべての 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	変更箇所
12.2(53)EX	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 ネットワーク内のカスタマーは、ネットワーク経由で多数の MAC アドレスをトンネリングし、使用可能な MAC アドレス テーブル スペースに入力できます。VLAN で MAC アドレス ラーニングを制御する場合、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。

MAC アドレス ラーニングは、1 つの VLAN (例: **no mac address-table learning vlan 223**) または一連の VLAN (例: **mac address-table learning vlan 1-10, 15**) でディセーブルにすることができます。

MAC アドレス ラーニング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 ラーニングをディセーブルにすると、ネットワークでフラッド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 ラーニング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 パケットをフラッドします。3 つ以上のポートを含む VLAN で MAC アドレス ラーニング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 ドメインでフラッドします。MAC アドレス ラーニング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 ラーニング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 ラーニング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 ラーニング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 ラーニング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。

mac address-table learning vlan

セキュアポートを含む VLAN で MAC アドレス ラーニング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 ラーニング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 ラーニング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 ラーニング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 ラーニ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 learning vlan 2003
```

すべての VLAN、または指定した VLAN の MAC アドレス ラーニング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 ラーニング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	変更箇所
12.2(53)EX	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。

■ mac address-table move update

関連コマンド

コマンド	説明
<code>clear mac address-table move update</code>	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。
<code>debug matm move update</code>	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。
<code>show mac address-table move update</code>	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。

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	変更箇所
12.2(53)EX	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 interface
gigabitethernet0/1
```

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	変更箇所
12.2(53)EX	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は、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 番め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。

macro apply

インターフェイスにマクロを適用するか、またはインターフェイスにマクロ設定を適用してこれを追跡するには、**macro apply** 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。

```
macro {apply | trace} macro-name [parameter {value}] [parameter {value}]
[parameter {value}]
```

構文の説明

apply	指定したインターフェイスにマクロを適用します。
trace	インターフェイスにマクロを適用し、そのマクロをデバッグするには、 trace キーワードを使用します。
<i>macro-name</i>	マクロ名を指定します。
parameter value	(任意) インターフェイスに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

macro trace macro-name 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実行されているマクロを適用および表示、あるいは構文または設定エラーを判別するためにマクロをデバッグできます。

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをインターフェイスに適用します。

一意の値の割り当てを必要とするマクロを作成する場合、**parameter value** キーワードを使用して、そのインターフェイスに固有の値を指定します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro apply macro-name ?** コマンドを使用すると、マクロに必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。

マクロをインターフェイスに適用する場合、マクロ名が自動的にインターフェイスに追加されます。

show running-configuration interface interface-id ユーザ EXEC コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

インターフェイスの範囲に適用されたマクロは、単一インターフェイスに適用されたマクロと同じ動作をします。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。1 つのインターフェイスでマクロ コマンドの実行に失敗しても、マクロは残りのインターフェイス上に適用されます。

インターフェイスで適用されたマクロの設定は、次のいずれかの方法で削除できます。

- **default interface interface-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（このコマンドによって、インターフェイス設定がデフォルト設定に戻ります）。
- マクロに含まれている各コマンドの **no** バージョンを入力する。
- マクロの **no** バージョンを適用する（**no** バージョンは一部のマクロには利用できません）。

例

macro name グローバル コンフィギュレーション コマンドを使用してマクロを作成したあとは、そのマクロをインターフェイスに適用できます。次の例では、**duplex** という名前のユーザ作成マクロをインターフェイスに適用する方法を示します。

```
Switch(config-if)# macro apply duplex
```

マクロをデバッグするには、**macro trace** 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、マクロがインターフェイスに適用されたときのマクロの構文または設定エラーを判別できます。次の例では、インターフェイス上の **duplex** という名前のユーザ作成マクロをトラブルシューティングする方法を示します。

```
Switch(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

関連コマンド

コマンド	説明
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro description

インターフェイスに適用されるマクロの説明を入力するには、**macro description** インターフェイス コンフィギュレーション コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

macro description *text*

no macro description

構文の説明

description *text* 指定したインターフェイスに適用されたマクロについての説明を入力します。

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	変更箇所
12.2(53)EX	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コメント テキストまたはマクロ名を関連付けるには、**description** キーワードを使用します。単一インターフェイスに複数のマクロを適用する場合、説明テキストは最後に適用したマクロのものになります。

次の例では、インターフェイスに説明を追加する方法を示します。

```
Switch(config-if)# macro description duplex settings
```

設定を確認するには、**show parser macro description** 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
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro global

スイッチにマクロを適用するか、またはスイッチにマクロ設定を適用してこれを追跡するには、**macro global** 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。

```
macro global {apply | trace} macro-name [parameter {value}] [parameter {value}]
[parameter {value}]
```

構文の説明

apply	スイッチにマクロを適用します。
trace	スイッチにマクロを適用してマクロをデバッグします。
<i>macro-name</i>	マクロ名を指定します。
parameter value	(任意) スイッチに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

macro trace macro-name グローバル コンフィギュレーション コマンドを使用して、スイッチ上で実行されているマクロを適用および表示、あるいは構文または設定エラーを判別するためにマクロをデバッグできます。

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをスイッチに適用します。

一意の値の割り当てを必要とするマクロを作成する場合、**parameter value** キーワードを使用して、そのスイッチに固有の値を指定します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro global apply macro-name ?** コマンドを使用すると、マクロに必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。

マクロをスイッチに適用する場合、マクロ名が自動的にスイッチに追加されます。**show running-configuration** ユーザ EXEC コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

スイッチで適用されたグローバル マクロの設定を削除するには、マクロ内にある各コマンドの **no** バージョンを入力するか、またはマクロの **no** バージョンを適用します。(no バージョンは一部のマクロには利用できません)。

例

macro name グローバル コンフィギュレーション コマンドを使用してマクロを作成したあとは、そのマクロをスイッチに適用できます。次の例では、**snmp** マクロを表示する方法、およびそのマクロを適用してホスト名をテスト サーバに設定し、IP precedence 値を 7 に設定する方法を示します。

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

-----
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

マクロをデバッグするには、**macro global trace** 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、マクロがスイッチに適用されたときのマクロの構文または設定エラーを判別できます。次の例では、**ADDRESS** パラメータ値が入力されなかったために `snmp-server host` コマンドが失敗した一方で、残りのマクロがスイッチに適用されていることを示します。

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...`snmp-server enable traps port-security'
Applying command...`snmp-server enable traps linkup'
Applying command...`snmp-server enable traps linkdown'
Applying command...`snmp-server host'
%Error Unknown error.
Applying command...`snmp-server ip precedence 7'
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro global description

スイッチに適用されるマクロの説明を入力するには、**macro global description** 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。説明を削除するには、このコマンドの **no** 形式を使用します。

macro global description text

no macro global description

構文の説明

description text スイッチに適用されたマクロについての説明を入力します。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチにコメント テキストまたはマクロ名を関連付けるには、**description** キーワードを使用します。複数のマクロがスイッチに適用されている場合、説明テキストは最後に適用されたマクロの説明になります。

次の例では、スイッチに説明を追加する方法を示します。

```
Switch(config)# macro global description udlld aggressive mode enabled
```

設定を確認するには、**show parser macro description** 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
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro name

設定マクロを作成するには、**macro 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。マクロ定義を削除するには、このコマンドの **no** 形式を使用します。

macro name *macro-name*

no macro name *macro-name*

構文の説明

macro-name マクロの名前

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

マクロには、最大 3000 文字を含めることができます。1 行に 1 つのマクロ コマンドを入力します。マクロを終了するには **@** 文字を使用します。マクロ内にコメント テキストを入力するには、行の先頭に **#** 文字を使用します。

ヘルプ文字列を使用してキーワードを指定し、マクロ内で必須キーワードを定義できます。**#macro keywords word** を入力してマクロで使用できるキーワードを定義します。スペースで分離することにより最大で 3 つのヘルプ スtring を入力できます。4 つのキーワードを入力した場合、最初の 3 つのみが表示されます。

マクロ名では、大文字と小文字が区別されます。たとえば、コマンド **macro name Sample-Macro** と **macro name sample-macro** は、2 つの別個のマクロとなります。

マクロを作成する際に、**exit** や **end** コマンド、または **interface interface-id** コマンドを使用してコマンド モードを変更しないでください。これらのコマンドを使用すると、**exit**、**end**、または **interface interface-id** に続くコマンドが異なるコマンド モードで実行されることがあります。

このコマンドの **no** 形式によって、マクロ定義のみが削除されます。マクロがすでに適用されているインターフェイスの設定には、影響はありません。**default interface interface-id** インターフェイス コンフィギュレーション コマンドを使用すれば、インターフェイスで適用されたマクロの設定を削除できます。また、元のマクロの対応するコマンドすべての **no** 形式を含む既存のマクロの **anti-macro** を作成できます。次に **anti-macro** をインターフェイスに適用します。

既存のマクロと同じ名前の新しいマクロを作成して、マクロを変更することができます。新規作成されたマクロは既存のマクロを上書きしますが、元のマクロが適用されたインターフェイスの設定には影響を与えません。

例 次の例では、デュプレックスモードおよび速度を定義するマクロを作成する方法を示します。

```
Switch(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
```

次の例では、**# macro keyword** でマクロを作成する方法を示します。

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

次の例では、インターフェイスにマクロを適用する前に、必須キーワード値を表示する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# macro apply test ?
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
```

```
Switch(config-if)# macro apply test $VLANID ?
WORD Value of first keyword to replace
```

```
Switch(config-if)# macro apply test $VLANID 2
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
```

```
Switch(config-if)# macro apply test $VLANID 2 $MAX ?
WORD Value of second keyword to replace
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

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。
<i>name</i>	パケットを照合するアクセス リストの名前です。
<i>number</i>	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	変更箇所
12.2(53)EX	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。構文情報については、『 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 』> 「 IP Services Commands 」を選択してください。
action	パケットが Access Control List (ACL; アクセス コントロール リスト) 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。構文情報については、『 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 』> 「 IP Services Commands 」を選択してください。
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 access-group

指定したアクセス コントロール リスト (ACL) に基づいて、クラス マップの一致基準を設定するには、**match access-group** 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。ACL 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*

no match access-group *acl-index-or-name*

構文の説明

<i>acl-index-or-name</i>	IP 標準または拡張 Access Control List (ACL) または MAC (メディア アクセス コントロール) 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。
--------------------------	--

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match access-group コマンドは、パケットがクラス マップで指定されたクラスに属しているかどうかを確認するための一致基準として使用する番号付きまたは名前付き ACL を指定します。

match access-group コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

match access-group 分類は、入力ポリシー マップ上でのみ使用できます。

例

次に、一致基準としてアクセス コントロール リスト *acl1* を使用するクラス マップ *class* を作成する例を示します。

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match access-group acl1
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。

match cos

レイヤ 2 サービス クラス (CoS) マーキングに基づいてパケットと一致するには、**match cos** 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。CoS 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 cos cos-list |
```

```
no match cos cos-list
```

構文の説明

cos-list 着信パケットに対して一致する 4 つまでの CoS 値からなるリストです。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。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match cos コマンドでは、一致基準として使用する CoS 値を指定します。この一致基準により、クラス マップによって指定されるクラスにパケットが属しているかどうかを判別されます。

match cos コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

CoS 値との一致は、レイヤ 2 VLAN タグ付きトラフィックを伝送するポート上でだけサポートされます。つまり、**cos** 分類は、IEEE 802.1Q トランク ポート上でだけ使用できます。

match cos 分類は、入力および出力のポリシー マップ内で使用できます。

例

次に、CoS 値が 1 および 4 のすべての着信トラフィックに一致するクラス マップ *class* を作成する例を示します。

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match cos 1 4
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。

match ip dscp

クラス的一致基準として特定の IPv4 DiffServ コードポイント (DSCP) 値を識別するには、**match ip dscp** 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 ip dscp dscp-list

no match ip dscp dscp-list

構文の説明

<i>ip-dscp-list</i>	着信パケットに対して一致する 8 つまでの IPv4 DSCP 値からなるリストです。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。また、よく使用される値にはニーモニック名を入力できます。 DSCP 値を指定するための他のオプションについては、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 QoS」の章を参照してください。
---------------------	--

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match ip dscp コマンドでは、一致基準として使用する DSCP 値を指定します。この一致基準により、クラス マップによって指定されるクラスにパケットが属しているかどうかは判別されます。

このコマンドはクラス マップで使用され、パケット上の特定の DSCP 値マーキングを識別します。この場合、DSCP 値はマーキングとしてだけ使用され、数学的な意味はありません。たとえば、DSCP 値 2 は 1 よりも大きくありませんが、単に値 2 でマーキングされたパケットが値 1 でマーキングされたパケットとは異なることを示しています。これらのマーキングされたパケットの扱いを定義するには、ポリシーマップ クラス コンフィギュレーション モードで QoS ポリシーを設定します。

match ip dscp コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

1 つの一致ステートメントで最大 8 つの DSCP 値を入力できます。たとえば、DSCP 値 0、1、2、3、4、5、6、または 7 が必要な場合は、**match ip dscp 0 1 2 3 4 5 6 7** コマンドを入力します。クラスに属するには、パケットは、指定されている IPv4 DSCP 値の 1 つだけ（すべてではなく）に一致している必要があります。

match ip dscp 分類は、入力および出力のポリシー マップ内で使用できます。

例 次に、DSCP 値が 10、11、および 12 のすべての着信トラフィックに一致するクラス マップ *inclass* を作成する例を示します。

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip dscp 10 11 12
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。

match ip precedence

クラス的一致基準として IPv4 precedence 値を識別するには、**match ip precedence** 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 ip precedence ip-precedence-list

no match ip precedence ip-precedence-list

構文の説明

ip precedence	着信パケットに対して一致する 4 つまでの IPv4 precedence 値からなるリスト
ip-precedence-list	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。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match ip precedence コマンドでは、一致基準として使用する IPv4 precedence 値を指定します。この一致基準により、クラス マップによって指定されるクラスにパケットが属しているかどうかを判別されます。

precedence 値はマーキングとしてだけ使用されます。この場合、IP precedence 値に数学的な意味はありません。たとえば、precedence 値 2 は 1 よりも大きくありませんが、単に値 2 でマーキングされたパケットが値 1 でマーキングされたパケットとは異なることを示しています。これらのマーキングされたパケットの扱いを定義するには、ポリシーマップ クラス コンフィギュレーション モードで QoS ポリシーを設定します。

match ip precedence コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

1 つの一致ステートメントで最大 4 つの IPv4 precedence 値を入力できます。たとえば、IP precedence 値 0、1、2、または 7 が必要な場合は、**match ip precedence 0 1 2 7** コマンドを入力します。クラスに属するには、パケットは、指定されている IP precedence 値の 1 つだけ（すべてではなく）に一致している必要があります。

match ip precedence 分類は、入力および出力のポリシー マップ内で使用できます。

例

次に、IP-precedence 値が 5、6、および 7 のすべての着信トラフィックに一致するクラス マップ *class* を作成する例を示します。

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip precedence 5 6 7
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。

match qos-group

クラス的一致基準として特定の Quality Of Service (QoS) グループ値を識別するには、**match qos-group** 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 qos-group value

no match qos-group value

構文の説明

qos-group value Quality Of Service グループ値。指定できる範囲は 0 ~ 99 です。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

match qos-group コマンドでは、一致基準として使用する QoS グループ値を指定します。この一致基準により、クラス マップによって指定されるクラスにパケットが属しているかどうかは判別されます。

QoS グループ値はマーキングとしてだけ使用され、数学的な意味はありません。たとえば、precedence 値 2 は 1 よりも大きくありませんが、単に値 2 でマーキングされたパケットが値 1 でマーキングされたパケットとは異なることを示しています。これらのマーキングされたパケットの扱いを定義するには、ポリシーマップ クラス コンフィギュレーション モードで QoS ポリシーを設定します。

QoS グループ値はスイッチ内に限定されます。つまり、パケットがスイッチから送出される時、パケットでマーキングされた QoS グループ値はスイッチから送出されません。パケットとともに残るマーキングが必要な場合は、IP DiffServ コード ポイント (DSCP) 値、IP precedence 値、またはパケット マーキングの別の方法を使用します。

match qos-group コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

match qos-group 分類は、出力ポリシー マップ上でのみ使用できます。

スイッチ (0 ~ 99) には、100 を超える QoS グループを指定することはできません。

例

次に、一致基準として QoS グループ 13 を使用してトラフィックを分類する例を示します。

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match qos-group 13
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
<code>class-map</code>	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。
<code>show class-map</code>	QoS クラス マップを表示します。

match vlan

所定のインターフェイスにユーザが指定した VLAN 上で伝送されるフレームに QoS ポリシーを適用するには、階層型ポリシー マップの親ポリシー内で **match vlan** 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。トランク ポートでの VLAN 単位の分類に階層型ポリシー マップを使用できます。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 vlan *vlan-list*

no match vlan *vlan-list*

構文の説明

vlan-list

着信パケットに対して一致する VLAN ID または VLAN 範囲を、トランク ポート上のポート単位、VLAN 単位 QoS 用の親ポリシー マップ内で指定します。VLAN ID は、30 個まで入力できます。VLAN の範囲を指定するには、ハイフンを使用します。1 つの VLAN 範囲は、2 つの VLAN ID として数えられます。個々の VLAN は、スペースを使用して区切ります。指定できる範囲は 1 ~ 4094 です。

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

変更箇所

12.2(53)EX

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、2 レベルの階層型入力ポリシー マップを使用する場合に限り、サポートされます。このポリシー マップは、親レベルで VLAN ベースの分類を定義し、子レベルで 1 つまたは複数の該当する VLAN に適用される QoS ポリシーを定義します。

親レベルで複数のサービス クラスを設定することにより、各種 VLAN の組み合わせを照合できます。また、子ポリシー マップを使用することにより、親サービス クラスごとに個別の QoS ポリシーを適用できます。

子ポリシー マップに関連付けられた 1 つまたは複数のクラスがあるポリシーは、親ポリシー マップと見なされます。親ポリシー マップ内の各クラスは、親クラスと呼ばれます。親クラスでは、**match vlan** コマンドだけを設定できます。子ポリシー マップ内のクラスでは、**match vlan** コマンドを設定できません。

ポート単位、VLAN 単位の親レベルのクラス マップでは、子ポリシー アソシエーションだけをサポートします。いずれのアクションも設定できません。さらに、親レベルのクラス マップでは、クラスの **class-default** のアクションまたは子ポリシー アソシエーションを設定できません。

子ポリシー マップ内では、レイヤ 2 とレイヤ 3 が混在するクラス マップを設定できません。このような子ポリシー マップを親ポリシーに関連付けようとすると、設定は拒否されます。ただし、レイヤ 2 とレイヤ 3 の子ポリシーを異なる親レベルのクラス マップに関連付けることはできます。

ポート単位、VLAN 単位 QoS は、IEEE 802.1Q トランク ポート上でだけサポートされます。

ポート単位、VLAN 単位の階層型ポリシーマップをインターフェイスに付加した後は、VLAN ベースの分類が含まれる親クラスを動的に追加または削除できません。そのような設定変更を行う前に、サービス ポリシーをインターフェイスから消去する必要があります。

VLAN または VLAN のセットに付加されている子ポリシー マップに、レイヤ 3 分類 (**match ip dscp**、**match ip precedence**、**match IP ACL**) だけが含まれる場合、これらの VLAN は、必ずポート単位、VLAN 単位ポリシーが付加されているポート上でだけ実行されることに注意する必要があります。この制限事項に従わない場合は、これらの VLAN 上のスイッチに着信するトラフィックの QoS 動作が不適切になる場合があります。

また、ポート単位 VLAN 単位が適用されるトランク ポート上で、**switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用して、VLAN メンバーシップを制限することも推奨します。レイヤ 3 分類が設定されたポート単位、VLAN 単位のポリシーが含まれるトランク ポート間で VLAN メンバーシップが重複した場合も、予期せぬ QoS 動作が発生する可能性があります。

match vlan コマンドを使用する前に、**class-map** 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、一致基準を設定するクラスの名前を指定する必要があります。

例

次の例では、子レベルのポリシー マップのクラス マップが音声およびビデオ トラフィックの一致基準を指定して、子ポリシー マップが各トラフィック タイプの入力ポリシングに対するアクションを設定します。親レベルのポリシー マップは、指定されたポート上の子ポリシー マップが適用される VLAN を指定します。

```
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```



(注) また、一致基準を **match vlan 100 200 300** と入力した場合でも、同じ結果になります。

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# set ip precedence 4
Switch(config-pmap-c)# exit
```

```
Switch(config)# policy-map parent-customer-1
Switch(config-pmap)# class customer-1-vlan
Switch(config-pmap-c)# service-policy ingress-policy-1
Switch(config-pmap-c)# 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。

■ match vlan

関連コマンド

コマンド	説明
class-map	指定したクラス名とパケットとの比較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

インターフェイスで Automatic Medium-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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスで 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、インターフェイスの速度とデュプレックスも **auto** に設定する必要があります。ポートがユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) の場合、**mdix auto** コマンドを使用する前に、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス (NNI) はデフォルトでイネーブルです。

接続された一方または両方のインターフェイスで **Auto-MDIX** を（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）イネーブルにすると、必要なケーブル タイプ（ストレートまたはクロス）が間違ってもリンクアップが発生します。

Auto-MDIX は、すべての 10/100-Mb/s インターフェイス上および 10/100/1000BASE-T/BASE-TX 小型フォーム ファクタ (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 gigabitethernet0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

■ mdix auto

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。

関連コマンド

コマンド	説明
show controllers ethernet-controller interface-id phy	Auto MDIX の動作ステートを含む、インターフェイスの内部レジスタに関する一般情報を表示します。

media-type

デュアルパーパス ポートのインターフェイスとタイプを手動で選択したり、最初にリンクが確立されたタイプをスイッチで動的に選択するように設定したりするには、**media-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。

```
media-type {auto-select | rj45 | sfp}
```

```
no media-type
```

構文の説明

auto-select	最初に確立されたリンクに基づいてタイプをスイッチで動的に選択できるようにします。
rj45	RJ-45 インターフェイスを選択します。
sfp	小型フォーム ファクタ (SFP) モジュール インターフェイスを選択します。

デフォルト

デフォルトでは、スイッチは動的にリンクを選択します (**auto-select**)

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

デュアルパーパス ポートの RJ-45 インターフェイスおよび SFP インターフェイスを同時に使用して、冗長リンクを提供することはできません。

auto-select を選択した場合、スイッチは最初にリンクが確立されたタイプを動的に選択します。これがデフォルトのモードです。スイッチはアクティブなリンクがダウンの状態になるまで、他のメディアタイプをディセーブルにします。アクティブなリンクがダウンの状態になると、いずれかのリンクがアップの状態になるまで、スイッチにより両方のタイプがイネーブル化されます。両方のメディアにアクティブ リンクがある場合、SFP リンクが優先されます。**auto-select** モードでは、スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます (デフォルト)。

rj45 を選択した場合、スイッチは SFP モジュール インターフェイスをディセーブルにします。ケーブルを SFP ポートに接続した場合、RJ-45 がダウンしているか切断されている場合でも、リンクを確立できません。このモードでは、デュアルパーパス ポートは 10/100/1000BASE-TX インターフェイスと同様の動作をします。このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。

sfp を選択した場合、スイッチは RJ-45 インターフェイスをディセーブルにします。このポートにケーブルを接続した場合、SFP モジュール側がダウンしている場合または SFP モジュールが存在しない場合であっても、リンクを確立できません。インストールされている SFP モジュールのタイプに基づいて、このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。

デュアルパーパス ポートの速度またはデュプレックスを設定するには、まずメディア タイプを選択する必要があります。**auto-select** を設定した場合、**speed** および **duplex** インターフェイス コンフィギュレーション コマンドによる設定は行えません。インターフェイス タイプを変更すると、速度およびデュプレックス設定は削除されます。スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます (デフォルト)。

メディア タイプが **auto-select** の場合、スイッチは次の基準を使用してメディア タイプを選択します。



(注) SFP は、光ファイバ ケーブルまたは銅線ケーブルを SFP モジュールに差し込むまでインストールされません。

- インストールされているメディア タイプがただ 1 つの場合、このインターフェイスはアクティブとなり、メディアが削除されるかスイッチがリロードされるまではアクティブのままです。
- イネーブルなデュアルパーパス ポートに両方のメディア タイプをインストールしている場合、スイッチは最初にインストールされたタイプに基づいてアクティブ リnkを選択します。
- 接続されている両方のケーブルでスイッチの電源を投入した場合、または **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 コマンドでデュアルパーパス アップリンク ポートをイネーブル化した場合、SFP モジュール インターフェイスが選択されます。これ以外の場合、最初にアップの状態になったリンクのタイプに基づいて、アクティブなリンクが選択されます。

例

次の例では、SFP インターフェイスを選択するよう設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# media-type sfp
```

設定を確認するには、**show interfaces interface-id capabilities** または **show interfaces interface-id transceiver properties** 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 capabilities	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の機能を表示します。
show interfaces transceiver properties	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の速度、デュプレックス、およびメディアタイプの設定を表示します。

monitor session

新規のスイッチドポートアナライザ (SPAN) セッションまたはリモート SPAN (RSPAN) 送信元/宛先セッションを開始し、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) の宛先ポート上で着信トラフィックをイネーブルにし、既存の SPAN または RSPAN セッションでインターフェイスや VLAN を追加/削除し、SPAN 送信元トラフィックを特定の VLAN に制限 (フィルタリング) 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。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の場合、**encapsulation dot1q** または **encapsulation replicate** キーワードは、このコマンドの **no** 形式では無視されます。

```
monitor session session_number destination {interface interface-id [, | -] [encapsulation
{dot1q | replicate}]} [ingress {[dot1q | untagged] 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 {dot1q | replicate}]} [ingress {[dot1q | untagged] 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

<i>session_number</i>	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。
interface <i>interface-id</i>	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 (タイプおよびポート番号を含む) 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。
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。
encapsulation replicate	(任意) カプセル化方式を指定します。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。 <ul style="list-style-type: none"> dot1q : IEEE 802.1Q カプセル化を指定します。 replicate : 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。 (注) 入力したこれらのキーワードは、ローカル SPAN にだけ有効です。RSPAN に対しては、RSPAN VLAN ID が元の 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 <i>vlan-id</i>	入力トラフィックのデフォルト VLAN として指定されている VLAN で IEEE 802.1Q 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 <i>vlan-id</i>	入力トラフィックのデフォルト VLAN として指定されている VLAN でタグなし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。
vlan <i>vlan-id</i>	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 <i>vlan-id</i>	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。 (注) 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 <i>vlan-id</i>	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。 <i>vlan-id</i> 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 <i>vlan-id</i>	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 dot1q** または **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	変更箇所
12.2(53)EX	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。

スイッチ上で、最大 64 の宛先ポートを保有できます。

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 IEEE 802.1x をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。(802.1x を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 をイネーブルにできません。

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。
- 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続くキーワードが、**dot1q**、**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）。
- **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続くキーワードが **dot1q**、**untagged** のいずれであるかによって決まります。

例

次の例では、ローカル SPAN セッション 1 を作成し、送信元ポート 1 から宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
```

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 gigabitethernet0/2
```

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 gigabitethernet0/1
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 gigabitethernet0/2
```

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 gigabitethernet0/2 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 gigabitethernet0/2 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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

mvr (グローバル コンフィギュレーション)

スイッチ上のマルチキャスト VLAN レジストレーション (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 | ringmode flood | vlan vlan-id]
```

```
no mvr [group ip-address | mode [compatible | dynamic] | querytime | ringmode flood | 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 ~ 2000 です。ただし、モードが compatible の場合、512 より大きい値を入力しても、スイッチで許可されるグループは 512 だけです。ダイナミック モードでは、2000 のグループをサポートします。デフォルトは 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 (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。

ringmode flood	(任意) アクセス リングの MVR リング モード フラッディングをイネーブルにします。このコマンドを入力して、リング環境で出力ポートのトラフィック フローを制御し、ユニキャスト トラフィックのドロップを防ぎます。
vlan <i>vlan-id</i>	(任意) MVR マルチキャスト データが受信される 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 (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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

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 モードが互換 (デフォルト) の場合は、512 個のマルチキャスト エントリ (MVR グループ アドレス) を設定できます。コマンド ラインのヘルプに表示される範囲は 1 ~ 2000 ですが、スイッチで許可されるグループは 512 だけです。

MVR モードがダイナミックの場合は、スイッチで最大 2000 の MVR グループ アドレスを設定できます。同時にアクティブなマルチキャスト ストリームの最大数 (受信できるテレビ チャンネルの最大数) は 512 です。この上限に達すると、*グループの最大ハードウェアの上限に達しました*、というメッセージが生成されます。IGMP 加入がポートにある場合や、**mvr vlan *vlan-id* group *ip-address*** インターフェイス コンフィギュレーション コマンドを入力して、ポートをグループに加入するように設定する場合、ハードウェア エントリが発生することに注意してください。

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 3500 XL スイッチと連携動作している場合は、それらの中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 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は、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。

Cisco IOS Release 12.2(52)SE 以降、**mvr ringmode flood** 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、リング トポロジでのデータ転送がメンバとして検出されたポートに制限され、マルチキャスト ルータ ポートへの転送が除外されるようにすることができます。これにより、MVR マルチキャスト トラフィックが一方向に流れ、ユニキャスト トラフィックが逆方向に流れる場合に、ユニキャスト トラフィックがリング環境でドロップされません。

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
```

設定済みの IP マルチキャスト グループ アドレスを表示するには、**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	設定済み MVR インターフェイスのタイプ、モード、VLAN、ステータス、即時脱退設定を表示します。また、インターフェイスがメンバーであるすべての MVR グループを表示できます。
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 のポートをマルチキャスト VLAN レジストレーション (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] [receiver
vlan vlan-id]}}
```

```
no mvr {immediate | type {receiver | source} | vlan vlan-id {[group ip-address] [receiver
vlan vlan-id]}}
```

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。 (注) トランク ポートを MVR レシーバ ポートとして設定する場合は、送信元ポートをネットワーク ノード インターフェイス (NNI) として、MVR トランク レシーバ ポートをユーザ ノード インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) として設定することを推奨します。
vlan vlan-id	システムの mvr vlan を指定します。
group 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、ポートまたは VLAN 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。
receiver vlan vlan-id	(任意) レシーバ VLAN を指定します。

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	変更箇所
12.2(53)EX	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。

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 gigabitethernet0/1
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 gigabitethernet0/1
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 gigabitethernet0/2
Switch(config-if)# mvr vlan1 group 228.1.23.4
```

次の例では、VLAN 100 のポート 2 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。この例では、受信ポートがアクセス ポートです。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan 100 group 228.1.23.4
```

次の例では、ポート 5 上で、レシーバ VLAN 201 を MVR VLAN 100 に追加する方法を示します。

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 receiver vlan 201
```

次に、100 の MVR VLAN の IP マルチキャスト グループ 239.1.1.1 のスタティック メンバとしてポート 5 でレシーバ VLAN 201 を追加する例を示します。

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
```

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)	スイッチ上でマルチキャスト VLAN レジストレーション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。

oam protocol cfm svlan

イーサネット仮想接続 (EVC) 運用管理および保守 (OAM) プロトコルを IEEE 801.2ag 接続障害管理 (CFM) として設定し、CFM ドメイン レベルのサービス プロバイダー VLAN-ID を識別するには、**oam protocol cfm svlan** EVC コンフィギュレーション コマンドを使用します。EVC の OAM プロトコル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。

oam protocol cfm svlan *vlan-id* domain *domain-name*

no oam protocol

構文の説明

<i>vlan-id</i>	CFM のサービス プロバイダー VLAN ID。指定できる範囲は 1 ~ 4094 です。
domain <i>domain-name</i>	サービス プロバイダー VLAN ID の CFM ドメインを識別します。CFM ドメインが存在しない場合は、コマンドが拒否され、エラー メッセージが表示されます。

デフォルト

EVC に識別されるサービス プロバイダー VLAN はありません。

コマンド モード

EVC コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

domain *domain-name* を入力する場合は、**ethernet cfm domain *domain-name* level *level-id*** グローバル コンフィギュレーション コマンドを入力して、CFM ドメインを事前に作成する必要があります。CFM ドメインが存在しない場合は、コマンドが拒否され、エラー メッセージが表示されます。

例

次の例では、EVC コンフィギュレーション モードを開始して、OAM プロトコルを CFM として設定する方法を示します。

```
Switch(config)# ethernet evc test1
Switch(config-etc)# oam protocol cfm svlan 22 domain Operator
```

関連コマンド

コマンド	説明
ethernet evc <i>evc-id</i>	EVC を定義し、EVC コンフィギュレーション モードを開始します。
ethernet cfm domain	CFM ドメインを定義し、ドメイン レベルを設定します。

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
```



(注) PAgP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

構文の説明

aggregation-port	論理ポート チャン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。チャンネルの一方の終端は、特定の宛先 MAC または IP アドレスのチャン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 チャンネル) 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスがユーザ ネットワーク インターフェイス (UNI) の場合、**pagp learn-method** を設定する前に、**port-type nni** または **port-type eni** 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。学習は、リンクの両端で同じ方式に設定する必要があります。



(注) コマンドライン インターフェイス (CLI) で **physical-port** キーワードを指定しても、Cisco CGS 2520 スイッチがサポートするのは、集約ポートでのアドレス ラーニングのみです。**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 コマンドはスイッチ ハードウェアに影響を及ぼしませんが、物理ポートによるアドレス ラーニングだけをサポートしているデバイスとの PAgP の相互運用性のために必要です。



(注)

Cisco CGS 2520 スイッチへのリンク パートナーが物理ラーナーの場合、物理ポート ラーナーとしてスイッチを設定することを推奨します。 **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、 **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 アドレスに基づく負荷分散方式を設定します。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 チャン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 チャンネル グループ情報を表示します。
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 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

pagp port-priority

EtherChannel を経由するすべての Port Aggregation Protocol (PAgP; ポート集約プロトコル) 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



(注)

PAgP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスがユーザ ネットワーク インターフェイス (UNI) の場合、**pagp port-priority** を設定する前に、**port-type nni** または **port-type eni** 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。

同じ EtherChannel 内で動作可能な最も高いプライオリティを持ち、メンバーシップを持つ物理ポートが、PAgP 送信用として選択されます。



(注)

コマンドライン インターフェイス (CLI) で **physical-port** キーワードを指定しても、Cisco CGS 2520 スイッチがサポートするのは、集約ポートでのアドレス ラーニングのみです。**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 コマンドはスイッチ ハードウェアに影響を及ぼしませんが、物理ポートによるアドレス ラーニングだけをサポートしているデバイスとの PAgP の相互運用性のために必要です。

Cisco CGS 2520 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。

■ pagp port-priority

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 チャンネル グループ情報を表示します。
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 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

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; アクセス コントロール 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。

```
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。

■ permit (ARP アクセス リスト コンフィギュレーション)

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	変更箇所
	12.2(53)EX	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 Access Control List (ACL; アクセス コントロール リスト) 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] [routing] [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] [routing] [sequence value] [time-range name]
```



(注) **flow-label** キーワードおよび **reflect** キーワードはコマンドラインのヘルプ スtringに表示されませんが、サポートされていません。

インターネット制御メッセージ プロトコル

```
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] [routing] [sequence value] [time-range
name]
```

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]
[routing] [sequence value] [syn] [time-range name] [urg]
```

ユーザ データグラム プロトコル

```
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}] [routing] [sequence value] [time-range
name]
```



(注) **flow-label** キーワードおよび **reflect** キーワードはコマンドラインのヘルプ スtringに表示されませんが、サポートされていません。

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

<i>protocol</i>	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。
<i>source-ipv6-prefix/prefix-length</i>	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。
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 <i>source-ipv6-address</i> 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。
<i>operator [port-number]</i>	(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。 <i>source-ipv6-prefix/prefix-length</i> 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。 <i>destination-ipv6-prefix/prefix-length</i> 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 <i>port-number</i> 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。
<i>destination-ipv6-prefix/prefix-length</i>	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。
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 <i>destination-ipv6-address</i> 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 DiffServ コードポイント値を照合します。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 <i>operator [port-number]</i> 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が、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。
routing	(任意) ルーティング拡張ヘッダーを持つパケットをマッチングします。
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) 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は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	変更箇所
12.2(53)EX	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、**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が、IPv6 専用です。

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。

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 ネイバー探索を許可します。ICMPv6 ネイバー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。3 つの暗黙的な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 ネイバー探索プロセスでは、IPv6 ネットワーク層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 ネイバー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 ネイバー探索プロセスと同等の Address Resolution Protocol (ARP) は、別のデータリンク層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 および *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 (送信元プレフィックスはトラフィックの送信元に基づいてトラフィックをフィルタリングし、送信先プレフィックスはトラフィックの送信先に基づいてトラフィックをフィルタリングします)。

このスイッチは、すべての範囲のプレフィクス長で IPv6 アドレス マッチングをサポートしています。

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 2001:0DB8:0300:0201::/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 gigabitethernet0/3
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（受信および送信）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	現在のすべての IPv6 アクセス リスト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 | larc-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 | larc-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tring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 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。 <ul style="list-style-type: none"> 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 <i>don't care</i> 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 <i>lsap-number mask</i>	(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。 <i>mask</i> は、照合を行う前に LSAP 番号に適用される <i>don't care</i> 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) Echo 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 2-4 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 2-4 IPX フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	フレーム タイプ	
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	変更箇所
12.2(53)EX	このコマンドが追加されました。

■ permit (MAC アクセス リスト コンフィギュレーション)

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; アクセス コントロール エントリ) 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。



(注)

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

分類したトラフィックにそれぞれポリサーを定義し、ポリシーマップ クラス ポリシング コンフィギュレーション モードを開始するには、**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、超過バースト伝送サイズ、および最大値を超過した場合の対処法を定義します。ポリシーマップ クラス ポリシング コンフィギュレーション モードでは、パケットに複数のアクションを指定できます。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。



(注) **police rate** キーワードおよび **percent** キーワードはコマンドラインのヘルプに表示されますが、サポートされていません。

```
police {cir cir-bps | rate-bps} [burst-bytes] | bc [burst-value] | pir pir-bps [be burst-bytes]
[conform-action [drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence]
[table table-map name]}] | set-dscp-transmit {new-dscp-value | [cos | dscp |
precedence] [table table-map name]}] | set-prec-transmit {new-precedence-value |
[cos | dscp | precedence] [table table-map name]}] | set-qos-transmit qos-group-value
| transmit] [exceed action [drop | set-cos-transmit {new-cos-value | [cos | dscp |
precedence] [table table-map name]}] | set-dscp-transmit {new-dscp-value | [cos |
dscp | precedence] [table table-map name]}] | set-prec-transmit
{new-precedence-value | [cos | dscp | precedence] [table table-map name]}] |
set-qos-transmit qos-group-value | transmit] [violate-action [drop | set-cos-transmit
{new-cos-value | [cos | dscp | precedence] [table table-map name]}] | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence] [table table-map name]}] |
set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map
name]}] | set-qos-transmit qos-group-value | transmit]]
```

```
no police {cir cir-bps | rate-bps} [burst-bytes] | bc [burst-value] | pir pir-bps [be
burst-bytes] [conform-action [drop | set-cos-transmit {new-cos-value | [cos | dscp |
precedence] [table table-map name]}] | set-dscp-transmit {new-dscp-value | [cos |
dscp | precedence] [table table-map name]}] | set-prec-transmit
{new-precedence-value | [cos | dscp | precedence] [table table-map name]}] |
set-qos-transmit qos-group-value | transmit] [exceed action [drop | set-cos-transmit
{new-cos-value | [cos | dscp | precedence] [table table-map name]}] | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence] [table table-map name]}] |
set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map
name]}] | set-qos-transmit qos-group-value | transmit] [violate-action [drop |
set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]}] |
set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map
name]}] | set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table
table-map name]}] | set-qos-transmit qos-group-value | transmit]]
```



(注) **priority** ポリシーマップ クラス コマンドで **police** を使用してプライオリティ キューを無条件にレート制限すると、バースト サイズの値はサポートされず、*rate-bps* 範囲がより小さくなります。デフォルトの適合アクション **transmit** とデフォルトの超過アクション **drop** だけがサポートされます。

構文の説明

cir	トラフィック ポリシングに使用される認定情報レート (CIR)。
<i>cir-bps</i>	bps 単位の CIR レート。指定できる範囲は 8000 ~ 1000000000 bps です。 (注) 出力サービス ポリシーの priority コマンドで police に指定できる範囲は 64000 ~ 1000000000 です。
<i>rate-bps</i>	平均トラフィック伝送速度を b/s で指定します。指定できる範囲は 8000 ~ 1000000000 です。 (注) 出力サービス ポリシーの priority コマンドで police に指定できる範囲は 64000 ~ 1000000000 です。
<i>burst-bytes</i>	(任意) 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。
bc [<i>burst-value</i>]	(任意) 適合バースト。許容バースト バイト数。指定できる範囲は 8000 ~ 1000000 バイトです。 バースト値を入力しない場合は、CIR レートで 250 ミリ秒 (ms) で送信できるバイト数と等しいバースト値が計算されます。通常、自動的に計算された値は適切です。すべての影響を理解している場合にのみ、新しい値を入力してください。
pir <i>pir-bps</i>	(任意) トラフィック ポリシングに使用する最大情報レート (PIR) です。指定できる範囲は 8000 ~ 1000000000 b/s です。
be <i>burst-bytes</i>	(任意) 拡張バースト。許容拡張バースト バイト数。 指定できる範囲は 8000 ~ 1000000 バイトです。
conform-action	(任意) CIR に適合する (CIR 以下の) パケットに実行するアクション。
drop	(任意) パケットをドロップします。 (注) 適合アクションが drop に設定されている場合、超過アクションおよび違反アクションは自動的に drop に設定されます。超過アクションが drop に設定されている場合、違反アクションは自動的に drop に設定されます。
set-cos-transmit <i>new-cos-value</i>	パケットの新しいサービス クラス (CoS) 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 CoS 値に指定できる範囲は 0 ~ 7 です。
set-dscp-transmit <i>new-dscp-value</i>	パケットの新しい DiffServ コードポイント (DSCP) 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 DSCP 値に指定できる範囲は 0 ~ 63 です。
set-prec-transmit <i>new-precedence-value</i>	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 IP precedence 値に指定できる範囲は 0 ~ 7 です。
set-qos-transmit <i>qos-group-value</i>	パケットの新しい Quality of Service (QoS) グループ値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 QoS 値に指定できる範囲は 0 ~ 99 です。
cos	(任意) 着信パケットの CoS 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
dscp	(任意) 着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
precedence	(任意) 着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。

table <i>table-map name</i>	(任意) 上記の <i>from-type</i> キーワードとともに使用します。拡張パケットマーキングに使用するテーブル マップを指定します。このテーブル マップを使用して、アクションの <i>from-type</i> パラメータに基づき、アクションの <i>to-type</i> がマーキングされます。
transmit	(任意) パケットを変更せずに送信します。
exceed-action	(任意) CIR を超過し、PIR 以下のパケットに実行するアクションです。
violate-action	(任意) PIR を超過するパケットに対して実行するアクション。

デフォルト

ポリサーは定義されません。適合バースト (**bc**) は、設定されている CIR で自動的に 250 ミリ秒に設定されます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

適合アクション マーキングを設定するには、拡張パケット マーキングを使用し、変更されていないパケットを送信する超過アクションを設定し、明示的な値を使用してマーキングして、拡張パケットマーキングのすべての組み合わせを使用します。拡張パケット マーキングによって、あらゆる着信 QoS マーキングおよびテーブル マップに基づく QoS マーキングが変更されます。また、スイッチは、同じクラスの複数の QoS パラメータのマーキングと適合アクション、超過アクション、および違反アクション マーキングの同時設定をサポートします。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。

スイッチは、最大 254 のポリサー プロファイルをサポートします。サポートされているポリサー インスタンスの数は 1024 - 1 で、スイッチ上の合計インターフェイス数より多い数です。複数インスタンスで同じプロファイルを適用できます。

- スwitchのすべてのポートに、256 のポート単位、VLAN 単位ポリシーマップ内の固有の VLAN 分類基準を指定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*VLAN label resources exceeded* というエラー メッセージが返されます。
- QoS ACE 分類リソース制限に達するまで、ポート単位およびポート単位、VLAN 単位のポリシーマップをスイッチのすべてのポートに付加できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、*TCAM resources exceeded* というエラー メッセージが返されます。
- CPU 保護がイネーブルになっている場合、ポートごとに設定できるポリサーは 45 だけです。 **no policer cpu uni all** 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 CPU 保護をディセーブルにし、スイッチをリロードすると、ポート当たり最大 64 のポリサーを設定できます。 **show policer cpu uni-eni {drop | rate}** 特権 EXEC コマンドを入力し、CPU 保護がイネーブルになっているかどうか確認できます。詳細については、 **policer cpu uni** コマンドを参照してください。
- CPU 保護をディセーブルにする際はこれらの制限事項について注意してください。

- CPU 保護をディセーブルにすると、ユーザ定義クラスに対してポートごとに最大 63 のポリサー（すべての 4 番目のポート上で 62）を、すべてのスイッチの `class-default` に対して 1 つのポリサーを設定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、`policer resources exceeded` というエラーメッセージが返されます。
- CPU 保護をディセーブルにすると、プラットフォームについてスイッチに最大 255 のポリサーを設定できます。この制限を超える原因となるような任意のポリシーへ付加や変更を行うと失敗となり、`policer resources exceeded` というエラーメッセージが返されます。
- CPU 保護をディセーブルにして、45 を超えるポリサーを持つポリシー マップを付加してから、CPU 保護を再度イネーブルにして、リロードした場合、CPU 保護には、ポートごとに 19 のポリサーが再度必要となります。リロード中、ポリサー 46 以降は、`policer resources exceeded` のエラー条件を満たすことになるので、これらのクラスに付加されるポリサーはありません。

ポリシングは、`priority` ポリシーマップ クラス コンフィギュレーション コマンドでプライオリティキューの帯域幅を削減するように設定された入力ポリシーまたは出力ポリシーだけでサポートされません。



(注)

出力ポリシーの `priority` コマンドで使用する場合、ポリシング レートの範囲は 64000 ~ 1000000000 bps です。ただし、コマンドラインインターフェイスのヘルプに表示される範囲は 8000 ~ 1000000000 です。範囲外のレートでは、出力サービス ポリシーを付加できません。

出力ポリシー マップは、元の値ではなく、アウトオブプロファイル トラフィックの変更された値にのみ一致する必要があります。

複数の適合アクションまたは超過アクションを設定するには、ポリシーマップ クラス ポリシング コンフィギュレーション モードを開始し、`conform-action`、`exceed-action`、および `violate-action` ポリシーマップ クラス ポリシング コンフィギュレーション コマンドを使用します。

`violate-action` を設定しない場合、デフォルトで違反クラスが超過アクションと同じアクションに割り当てられます。

ポリサーを定義し、Enter キーを押すと、複数のポリシング アクションを設定できるポリシーマップ クラス ポリシング コンフィギュレーション モードが開始されます。

- **conform-action** : CIR に適合する (CIR 以下の) パケットで実行するアクション。デフォルトのアクションは、パケットの送信です。詳細については、`conform-action` ポリシーマップ クラス `police` コマンドを参照してください。
- **exceed-action** : CIR を超過し、PIR 以下のパケットに実行するアクション。デフォルトのアクションは、パケットのドロップです。詳細については、`exceed-action` ポリシーマップ クラス `police` コマンドを参照してください。
- **violate-action** : PIR を超過するパケットで実行するアクション。デフォルトのアクションは、パケットのドロップです。詳細については、`violate-action` ポリシーマップ クラス `police` コマンドを参照してください。
- **exit** : QoS ポリシーマップ クラス ポリシング コンフィギュレーション モードを終了します。複数のアクションを設定しない場合、他のポリシーマップ クラス `police` コマンドを入力しないで `exit` を入力できます。
- **no** : コマンドを無効にするか、デフォルトに設定します。

例

次に、バースト サイズが 20 KB の 1-Mb/s 平均レートでポリサーを設定する例を示します。ポリサーは、パケットがレートに準拠している場合は新しい DSCP precedence 値を設定し、トラフィックがレートを超過した場合はパケットをドロップします。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class inclass1
Switch(config-pmap-c)# police cir 1000000 20000 conform-action set-dscp-transmit 46
exceed-action drop
Switch(config-pmap-c)# exit
```

次に、ポリシーマップ コンフィギュレーション モードを使用して 2-rate、3-color ポリシングを設定する例を示します。

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000 conform-action transmit
exceed-action set-dscp-transmit 24 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

次に、ポリシーマップ クラス ポリシング コンフィギュレーション モードで同じ設定を作成する例を示します。

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
conform-action	CIR または PIR を満たし、レートが適合バーストよりも低いパケットのポリシーマップ クラスに対して複数のアクションを定義します。
exceed-action	CIR または PIR を超過し、適合値と超過バーストの間のレートを持つパケットのポリシーマップ クラスに対して複数のアクションを定義します。
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。
violate-action	CIR および PIR を超過し、適合レート + 超過バーストを超過するレートを持つパケットのポリシーマップ クラスに対して複数のアクションを定義します。
show policy-map	QoS ポリシー マップを表示します。

policer aggregate (グローバル コンフィギュレーション)

集約ポリサーを作成して、入力ポリシー マップ内の複数のクラスにおけるすべてのトラフィックのポリシングを行うには、**policer aggregate** 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、同一ポリシー マップ内の複数のクラスで共有できます。ポリサーは、最大許容伝送速度または認定情報レート、最大バースト伝送サイズ、および最大値に達するか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。

```
policer aggregate aggregate-policer-name {rate-bps | cir cir-bps} [bc burst-value] [pir
pir-bps [be burst-bytes]] [conform-action [drop | set-cos-transmit {new-cos-value |
[cos | dscp | precedence] [table table-map name]}] | set-dscp-transmit {new-dscp-value
| [cos | dscp | precedence] [table table-map name]}] | set-prec-transmit
{new-precedence-value | [cos | dscp | precedence] [table table-map name]}] |
set-qos-transmit qos-group-value | transmit] [exceed-action [drop | set-cos-transmit
{new-cos-value | [cos | dscp | precedence] [table table-map name]}] | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence] [table table-map name]}] |
set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map
name]}] | set-qos-transmit qos-group-value | transmit] [violate-action [drop |
set-cos-transmit {new-cos-value | [cos | dscp | precedence]}] | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence]}] | set-prec-transmit
{new-precedence-value | [cos | dscp | precedence]}] | set-qos-transmit qos-group-value
| transmit]]
```

```
no policer aggregate aggregate-policer-name {rate-bps | cir cir-bps} [bc burst-value] [pir
pir-bps [be burst-bytes]] [conform-action [drop | set-cos-transmit {new-cos-value |
[cos | dscp | precedence] [table table-map name]}] | set-dscp-transmit {new-dscp-value
| [cos | dscp | precedence] [table table-map name]}] | set-prec-transmit
{new-precedence-value | [cos | dscp | precedence] [table table-map name]}] |
set-qos-transmit qos-group-value | transmit] [exceed action [drop | set-cos-transmit
{new-cos-value | [cos | dscp | precedence] [table table-map name]}] | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence] [table table-map name]}] |
set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map
name]}] | set-qos-transmit qos-group-value | transmit] [violate-action [drop |
set-cos-transmit {new-cos-value | [cos | dscp | precedence]}] | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence]}] | set-prec-transmit
{new-precedence-value | [cos | dscp | precedence]}] | set-qos-transmit qos-group-value
| transmit]]
```

構文の説明

<i>aggregate-policer-name</i>	集約ポリサーの名前です。
<i>rate-bps</i>	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。
<i>cir cir-bps</i>	認定情報レート (CIR) (b/s)。指定できる範囲は、8000 ~ 1000000000 b/s です。

bc burst-value	(任意) 適合バースト。許容バースト バイト数。指定できる範囲は 8000 ~ 1000000 バイトです。 バースト値を入力しない場合は、CIR レートで 250 ミリ秒 (ms) で送信できるバイト数と等しいバースト値が計算されます。通常、自動的に計算された値は適切です。すべての影響を理解している場合にのみ、新しい値を入力してください。
pir pir-bps	(任意) トラフィック ポリシングに使用する最大情報レート (PIR) です。指定できる範囲は 8000 ~ 1000000000 b/s です。
be burst-bytes	(任意) 拡張バースト。許容拡張バースト バイト数。指定できる範囲は 8000 ~ 1000000 バイトです。
conform-action	(任意) CIR に適合する (CIR 以下の) パケットに実行するアクション。
drop	(任意) パケットをドロップします。 (注) 適合アクションが drop に設定されている場合、超過アクションおよび違反アクションは自動的に drop に設定されません。超過アクションが drop に設定されている場合、違反アクションは自動的に drop に設定されます。
set-cos-transmit cos-value	パケットの新しいサービスクラス (CoS) 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 CoS 値に指定できる範囲は 0 ~ 7 です。
set-dscp-transmit dscp-value	パケットの新しい DiffServ コードポイント (DSCP) 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 DSCP 値に指定できる範囲は 0 ~ 63 です。
set-prec-transmit precedence-value	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 IP precedence 値に指定できる範囲は 0 ~ 7 です。
set-qos-transmit qos-group-value	パケットの新しい Quality of Service (QoS) グループ値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 QoS 値に指定できる範囲は 0 ~ 99 です。
cos	(任意) 着信パケットの CoS 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
dscp	(任意) 着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
precedence	(任意) 着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケット マーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
table table-map name	(任意) 上記の <i>from-type</i> キーワードとともに使用します。拡張パケット マーキングに使用するテーブル マップを指定します。このテーブル マップを使用して、アクションの <i>from-type</i> パラメータに基づき、アクションの <i>to-type</i> がマーキングされます。 (注) テーブル マップは、違反アクションでサポートされません。
transmit	(任意) パケットを変更せずに送信します。

policer aggregate (グローバル コンフィギュレーション)

exceed-action	(任意) CIR を超過し、PIR 以下のパケットに実行するアクションです。
violate-action	(任意) PIR を超過するパケットに対して実行するアクション。

デフォルト

集約ポリサーは定義されません。

集約ポリサーを設定すると、適合バースト (**bc**) は、設定されている CIR で自動的に 250 ミリ秒に設定されます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

適合アクション マーキングを設定するには、拡張パケット マーキングを使用し、変更されていないパケットを送信する超過アクションと違反アクションを設定し、明示的な値を使用してマーキングして、拡張パケット マーキングのすべての組み合わせを使用します。拡張パケット マーキングによって、あらゆる着信 QoS マーキングおよびテーブル マップに基づく QoS マーキングが変更されます。また、スイッチは、同じクラスの複数の QoS パラメータのマーキングと適合アクション、超過アクション、および違反アクション マーキングの同時設定をサポートします。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。

violate-action を設定しない場合、デフォルトで違反クラスが**超過アクション**と同じアクションに割り当てられます。

スイッチでは、最大 254 の一意の集約ポリサーをサポートしています。

集約ポリシングは、入力ポリシー マップでだけサポートされます。

exceed-action のテーブル マップを設定し、違反アクションのアクションが明示的に設定されていない限り、集約ポリシングの **violate-action** に対するテーブル マップはサポートされません。

複数の適合、超過、違反アクションを集約ポリサーに **policer aggregate** グローバル コンフィギュレーション コマンドのパラメータとして同時に設定できますが、次の順序でアクションを入力する必要があります。

- **drop**、または **transmit** あるいは **set** アクションは、**conform-action** のあとに次の順序で入力する必要があります。

set-qos-transmit

set-dscp-transmit または **set-prec-transmit**

set-cos-transmit

- **drop**、**transmit** または **set** アクションは、**exceed-action** のあとに次の順序で入力する必要があります。

set-qos-transmit

set-dscp-transmit または **set-prec-transmit**

set-cos-transmit

- **drop**、**transmit** または **set** アクションは、**violate-action** のあとに次の順序で入力する必要があります。

set-qos-transmit**set-dscp-transmit** または **set-prec-transmit****set-cos-transmit**

出力ポリシー マップは、元の値ではなく、アウトオブプロファイル トラフィックの変更された値にのみ一致する必要があります。

集約ポリサーを設定すると、特定のバースト サイズおよび適合アクションと超過アクションを設定できます。バースト サイズ (**bc**) を指定しない場合は、CIR レートで 250 ミリ秒で送信できるバイト数と等しい適切なバースト サイズ値が計算されます。通常、自動的に計算された値は適切です。すべての影響を理解している場合にのみ、新しい値を入力してください。

例

次に、*agg-pol-1* という名前の集約ポリサーを設定し、ポリシー マップ内の複数のクラスに付加する例を示します。

```
Switch(config)# policer aggregate agg-pol-1 10900000 80000 exceed-action drop
Switch(config)# class-map test1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map test2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy map testexample
Switch(config-pmap)# class test1
Switch(config-pmap-c)# police aggregate agg-pol-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class test2
Switch(config-pmap-c)# police aggregate agg-pol-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

次に、2-rate、3-color 集約ポリサーを作成し、ポリシー マップ内の複数のクラスに付加する例を示します。ポリシー マップは入力ポートに結合されます。

```
Switch(config)# policer aggregate example cir 10900000 pir 80000000 conform-action
transmit exceed-action drop violate-action drop
Switch(config)# class-map testclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map testclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# class testclass2
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
```

■ **policer aggregate** (グローバル コンフィギュレーション)

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

設定を確認するには、**show 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
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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 policer aggregate	集約ポリサーの設定を表示します。

police aggregate (ポリシーマップクラス コンフィギュレーション)

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチ上では、ポートに関連付けられた最大 229 のポリサー インスタンスがサポートされます (228 のユーザ設定可能なポリサーと、1 つの内部使用に予約されたポリサー)。CPU 保護がイネーブルになっている場合 (デフォルト)、ポート当たり 45 の入力ポリサーを設定できます。 **no policer cpu uni all** 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て CPU 保護をディセーブルにすると、ユーザ定義クラスにはポート当たり最大 64 の入力ポリサー (すべての 4 番目のポート上で 63 ポリサー) を設定できます。詳細については、**policer cpu uni** コマンドを参照してください。

集約ポリシングは、入力ポリシー マップにだけ適用されます。

集約ポリサーは、個別のポリサーとは異なり、ポリシー マップ内の複数のトラフィック クラスで共有されます。インターフェイスに適用されたポリシー マップ内の複数のクラスにおけるトラフィック ストリームをポリシングするには、集約ポリサーを使用します。集約ポリシングは、複数のインターフェイス上のトラフィック ストリームの集約には使用できません。

1 つのポリシー マップだけが、任意の特定の集約ポリサーを使用できます。

例

次に、集約ポリシングをデフォルトのアクションを使用して設定し、同じポートのすべてのクラスに適用する例を示します。

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class in-class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
```

■ police aggregate (ポリシーマップクラス コンフィギュレーション)

```
Switch(config-pmap) # class in-class2
Switch(config-pmap-c) # police aggregate agg_policer1
Switch(config-pmap-c) # exit
Switch(config-pmap) # class in-class3
Switch(config-pmap-c) # police aggregate agg_policer1
Switch(config-pmap-c) # exit
```

設定を確認するには、**show 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
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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 policer aggregate	集約ポリサーの設定を表示します。

policer cpu uni

CPU 保護をイネーブルまたはディセーブルにし、スイッチのすべてのユーザ ネットワーク インターフェイス (UNI) および拡張ネットワーク インターフェイス (ENI) の CPU ポリシングしきい値を設定するには、**policer cpu uni** 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。デフォルトレートに戻す場合、または CPU 保護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。

```
policer cpu uni {all | rate-bps}
```

```
no policer cpu uni {all | rate-bps}
```

構文の説明

all	CPU 保護をイネーブルまたはディセーブルにするには、このキーワードを入力します。CPU 保護をディセーブルにすると、ポートごとに 45 ではなく 64 のポリサーを設定できます。
rate-bps	CPU ポリシングしきい値をビット/秒 (b/s) で指定します。指定できる範囲は 8000 ~ 409500 です。

デフォルト

CPU 保護がイネーブルになります。デフォルトのポリシングしきい値は 160000 b/s 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

偶発的または意図的な CPU 過負荷から保護するために、スイッチでは UNI および ENI の事前定義された 1 組のレイヤ 2 制御パケットおよび一部のレイヤ 3 制御パケットをドロップまたはレート制限することにより、自動的に CPU 保護またはコントロールプレーン セキュリティを実現します。スイッチは、CPU 保護のため、0 ~ 26 の番号が指定された 27 のコントロールプレーンのセキュリティ ポリサーを事前に割り当てます。ポリサー 26 は、廃棄ポリサーを意味します。ポリサー 0 ~ 25 は、ポートが制御プロトコルのレート制限ポリサーを使用することを意味します。

CPU ポリサーは事前に割り当てられています。**policer cpu uni rate-bps** コマンドを使用してレート制限しきい値だけを設定できます。設定されたしきい値は、すべての制御プロトコルおよびすべての UNI と ENI 適用されます。

CPU 保護ポリシングは、ポートごとに 19 のポリサーを使用します。これにより、ポートに最大 45 の入力ポリサーを付加することができます。ポートで 45 を超えるポリサーが必要な場合、45 を超えるポリサーを持つポリシー マップを付加する前に、**no cpu policer uni all** 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、CPU 保護をディセーブルにできます。CPU 保護をディセーブルにする、ポートに最大 64 の入力ポリサーを付加できます。

- CPU 保護をディセーブルにして、45 を超えるポリサーを持つポリシー マップを付加してから、CPU 保護を再度イネーブルにして、リロードした場合、CPU 保護には、ポートごとに 19 のポリサーが再度必要となります。リロード中、ポリサー 46 以降は、*policer resources exceeded* のエラー条件を満たすことになるので、これらのクラスに付加されるポリサーはありません。

policer cpu uni



(注) スイッチの各 4 ポート（ポート 1～4、5～8 など）では、最初の 3 ポートは、64 のポリサーをサポートしますが、4 番目のポートは、63 のポリサーだけをサポートできます。

CPU 保護機能をディセーブルまたはイネーブルにする場合、設定が反映される前に **reload** 特権 EXEC コマンドを入力することによって、スイッチをリロードする必要があります。



(注) CPU 保護をオフにするとプロトコル パッケージが CPU に到達可能となり、これが、CPU 処理の過負荷や、ソフトウェアによるストーム制御の原因となる可能性があります。

show policer cpu uni-eni {drop | rate} 特権 EXEC コマンドを入力し、CPU 保護がイネーブルになっているかどうか確認できます。

コントロールプレーン セキュリティの詳細については、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

次に、CPU 保護しきい値を 10000 b/s に設定し、その設定を確認する例を示します。

```
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policer cpu uni 10000
Switch(config)# end
```

設定を確認するには、**show policer cpu uni-eni rate** 特権 EXEC コマンドを入力します。

次に、CPU 保護をディセーブルにしてスイッチをリロードする例を示します。

```
Switch(config)# no policer cpu uni all
Switch(config)# end
Switch# reload
Proceed with reload? [confirm]
```

次に、CPU 保護がディセーブルの場合の **show policer cpu uni-eni rate** 特権 EXEC コマンドの出力例を示します。

```
Switch# show policer cpu uni-eni rate
CPU Protection feature is not enabled
```

関連コマンド

コマンド	説明
show policer cpu uni-eni rate	コントロールプレーン セキュリティ用に設定されたポリサーしきい値を表示します。

policy-map

複数の物理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 マップを削除する場合は、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。デフォルトでは、パケットは変更せずに送信されます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチでは、最大 256 の一意のポリシー マップをサポートしています。

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。

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 モードになり、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** : ポリシーのアクションが適用される指定トラフィック分類。分類は、**class-map** 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ます。詳細については、**class-map** コマンド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 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。



(注)

no policy-map コンフィギュレーション コマンドまたは **no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシー マップを削除する場合、ポリシー マップが消去されているインターフェイスの一覧を示す警告メッセージが表示されます。ポリシー マップは消去および削除されます。次に例を示します。

Warning: Detaching Policy test1 from Interface GigabitEthernet0/1

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。クラスの一貫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。

入力ポリシー マップおよび出力ポリシー マップを作成し、ポートに、入力ポリシー マップおよび出力ポリシー マップを 1 つずつ割り当てることができます。入力ポリシー マップは、ポート上の着信トラフィックに作用します。出力ポリシー マップは、発信トラフィックに作用します。

複数の物理ポートに対して、同一のポリシーマップを適用することができます。

入力ポリシー マップの設定を行うときは、次の注意事項に従ってください。

- スイッチのインターフェイスに付加できる入力ポリシー マップの合計数は、ハードウェア リソースの可用性により制限されます。いずれかのハードウェア リソースの制限を超過する入力ポリシー マップを付加しようとすると、設定エラーになります。
- 入力ポリシー マップの最大クラス マップ数は **64 + class-default** です。
- 1 つのポリシー マップ内の IP (IP 標準および拡張 ACL、DSCP または IP precedence) と非 IP (MAC ACL または CoS) 分類を 1 つのクラス マップ内、またはポリシー マップ内のクラス マップにわたって設定することはできません。
- **service-policy input** 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インターフェイスに入力ポリシー マップを付加した後に、入力ポリシー マップをインターフェイスから取り外さずに変更できます。分類基準、クラス、またはアクションの追加または削除、もしくは設定されたアクション (ポリサー、レート、マッピング、マーキングなど) のパラメータの変更を行うことができます。
- **match qos-group** コマンド、クラスベース均等化キューイング (CBWFQ) の **bandwidth** コマンド、クラスベース プライオリティ キューイングの **priority** コマンド、重み付きテール ドロップ (WTD) の **queue-limit** コマンド、ポート シェーピングの **shape average** コマンド、クラスベーストラフィック シェーピングは、入力ポリシー マップでサポートされていません。

出力ポリシー マップの設定を行うときは、次の注意事項に従ってください。

- 出力ポリシー マップには、最大 4 つのクラス (1 つは **class-default**) を含めることができます。
- スイッチは、スイッチ上の各ポートに固有の出力ポリシー マップの設定および付加をサポートしています。ただし、これらの出力ポリシー マップには、それぞれキュー制限を 3 つしか設定できません。これら 3 つの固有のキュー制限設定は、スイッチ ポート数に応じた数の出力ポリシー マップに含めることができます。4 つ目のキュー制限設定を含む出力ポリシー マップを付加しようとすると、エラー メッセージが表示され、付加は許可されません。帯域幅、プライオリティ、またはシェーピングの設定には制限はありません。
- すべての出力ポリシー マップには、同じ数のクラス マップ (1 ~ 3) と同じ分類 (つまり、同じクラス マップ) を含める必要があります。
- **service-policy output** 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に出力ポリシー マップを付加した後は、設定済みアクションのパラメータ (レート、パーセンテージなど) を変更すること、または、インターフェイスにポリシー マップが付加されている場合にクラス マップの分類基準を追加または削除することのみができます。クラスまたはアクションを追加、削除するには、すべてのインターフェイスからポリシー マップを消去して、変更し、再度インターフェイスに付加する必要があります。
- **match access-group** コマンド、マーキングの **set** コマンド、および **priority** コマンドを含まないポリシングの **police** コマンドは、出力ポリシー マップでサポートされていません。

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 ガイドを参照してください。

例

次に、3つのクラスの入力ポリシー マップを作成する例を示します。

```
Switch(config)# policy-map input-all
Switch(config-pmap)# class gold
Switch(config-pmap-c)# set dscp af43
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
```

次に、レート制限が gold クラスのプライオリティを指定し、残りの帯域幅の少なくとも 20% を silver クラスに、10% を bronze クラスに保証する出力ポリシー マップを設定する例を示します。

```
Switch(config)# policy-map output-2
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
```

次の例では、ポリシー マップ *output-2* を削除する方法を示します。

```
Switch(config)# no policy-map output-2
```

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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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 (インターフェイス コンフィギュレーション)	ポートにポリシー マップを適用します。
show policy-map	Quality of Service (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ン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、チャン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	変更箇所
12.2(53)EX	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 チャンネルへのアクセスや、ポート チャンネルの作成を行います。
show etherchannel	チャンネルの EtherChannel 情報を表示します。
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 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

port-type

既存のポートタイプからネットワーク ノード インターフェイス (NNI)、ユーザ ネットワーク インターフェイス (UNI)、または拡張ネットワーク インターフェイス (ENI) にポート タイプを変更するには、**port-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。ポートをデフォルト値設定に戻すには、このコマンドの **no** 形式を使用します。

```
port-type {eni | nni | uni}
```

```
no port-type
```

構文の説明

eni	拡張ネットワーク インターフェイス。ENI は、デフォルト設定が UNI と同じですが、設定により Cisco Discovery Protocol (CDP)、スパニング ツリー プロトコル (STP)、リンク層検出プロトコル (LLDP)、および EtherChannel のリンク集約制御プロトコル (LACP) またはポート集約プロトコル (PAgP) 用のプロトコル制御パケットをサポートできます。
nni	ネットワーク ノード インターフェイス。
uni	ユーザ ネットワーク インターフェイス。

デフォルト

コンフィギュレーション ファイルが存在しない場合は、すべての 10/100 ポートは、UNI で、小型フォーム ファクタ (SFP) モジュール スロットは NNI です。ポートは、ENI ポートとなるように設定します。

ENI として設定されたポートに UNI ポートと同じデフォルトがあっても、ENI の制御プロトコル (CDP、STP、LLDP、LACP と PAgP) を設定できます。これらのプロトコルは、UNI ではサポートされていません。

UNI または ENI のデフォルト ステータスは、スイッチを設定する場合に無許可のユーザが他のポートにアクセスするのを防止するため、管理上のダウンとなっています。これを設定する前に、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用して、UNI または ENI をイネーブルする必要があります。

NNI のデフォルト ステータスは管理上アップであり、サービス プロバイダーは初期設定時にリモートスイッチへのアクセスを許可されます。

ポートを ENI として設定すると、ポートの管理ステートは変わりません。ポートタイプの変更前にポート ステートが **シャットダウン** の場合は、**シャットダウン** ステートのままとなります。ステートが **シャットダウン** 以外の場合は **シャットダウン** 以外のステートのままとなります。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポートが別のポート タイプに再設定できます。別のインターフェイス タイプとして再設定されるポートは、現在のインターフェイス タイプの特性をすべて継承します。デフォルトでは、スイッチのすべてのポートは、UNI または NNI です。すべてのポートは常に、UNI、NNI、または ENI です。

一部の機能は、すべてのポートタイプでだけサポートされされていません。制御プロトコル (CDP、STP、LLDP、EtherChannel LACP および PAgP) のサポートは、ポートタイプによって異なります。

- NNI では、これらの機能はデフォルトでイネーブルになっています。
- ENI 上では、これらの機能はデフォルトでディセーブルになっていますが、コマンドライン インターフェイスを使用して、イネーブルにできます。
- これらの機能は、UNI ではサポートされていません。

特定の機能のサポートについては、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。1 つのタイプから別のタイプにポートを変更する場合、特定のインターフェイスの設定オプションの矛盾を防ぐために、ポートタイプに特化した機能が設定から削除されます。

スイッチのすべてのポートは UNI または ENI にすることができますが、スイッチでメトロ アクセス イメージが稼動している場合、4 つのポートを同時に NNI にすることができます。スイッチでメトロ IP アクセス イメージが稼動している場合、すべてのポートを NNI として設定できます。

no port-type インターフェイス コンフィギュレーション コマンドまたは **default port-type** インターフェイス コンフィギュレーション コマンドを入力すると、ポートがデフォルト ステート (ファストイーサネット ポートの場合は UNI、ギガビットイーサネット ポートの場合は NNI) に戻ります。

トラフィックは UNI または ENI の間ではスイッチングされません。また、UNI または ENI に着信するすべてのトラフィックは、ユーザが別のユーザのプライベート ネットワークにアクセスするのを防止するため、NNI から発信される必要があります。スイッチ内でトラフィックを 2 つ以上の UNI または ENI により交換するのが適切であれば、インターフェイスをコミュニティ VLAN に割り当てることができます。コミュニティ VLAN には、最大 8 つの UNI または ENI を含めることができます。同じコミュニティ VLAN に UNI および ENI を混在させることは推奨しません。

VLAN 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 ガイドを参照してください。

例

次の例では、ポートを NNI に変更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 fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type nni
5d20h: %SYS-5-CONFIG_I: Configured from console by console
Switch(config-if)# end
Switch# copy running-config startup-config
```

次の例では、ポートタイプを ENI に変更する方法を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type eni
Switch(config-if)# end
```

関連コマンド

コマンド	説明
no shutdown	インターフェイスをイネーブルにします。
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。
show port-type	インターフェイスのポートタイプを表示します。

power inline

Power over Ethernet (PoE) ポート上で電力管理モードを設定するには、スイッチで **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] | port maximum | static
[max max-wattage]}
```

```
no power inline {auto | never | police | port | 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 mW 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。
police [action log]	リアルタイムの消費電力のポリシングをイネーブルにします。これらのキーワードの詳細については、 power inline police コマンドを参照してください。
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)。
port maximum	ポートの最大電力レベル値 (20 W まで) を設定します。

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 mW です。

コマンド デフォルト

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	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 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 gigabitethernet1/0/1
Switch(config-if)# power inline auto
^
% Invalid input detected at '^' marker.
```

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 バジレットに送られます。



(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、スイッチはクラス 0 またはクラス 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** 特権 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。



(注) Cisco IOS Release 12.2(53)EX 以降のリリースでは、拡張 PoE がサポートされます。**power inline port maximum** 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、最大電力レベルが 20 ワットのデバイスをサポートできます。

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。不正なリンクアップが生じ、ポートが **errdisable** ステートになる可能性があります。

power inline never コマンドで設定したポートにシスコの受電装置を接続しないでください。

例

次の例では、スイッチ上で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 gigabitethernet1/0/2
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、スイッチ上で PoE ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
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、スイッチ上で 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 gigabitethernet1/0/2
Switch(config-if)# power inline never
```

次の例では、接続されたデバイスに 20 W を提供するようにポートを設定する方法を示します。

```
Switch(config-if)# power inline port maximum 20000
```

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。



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 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.
It is recommended to enable power policing if the switch supports it.
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。

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 mW 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.
It is recommended to enable power policing if the switch supports it.
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 mW 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 gigabitethernet1/0/2
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.
It is recommended to enable power policing if the switch supports it.
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 inline police

リアルタイム電力消費のポリシングをイネーブルにするには、スイッチで **power inline police** 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。

power inline police [action log]

no power inline police

構文の説明

action log	(任意) リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、スイッチは接続された装置に電力を供給しながら Syslog メッセージを生成します。 action log キーワードを入力しない場合に、リアルタイムの電力消費がポートの最大電力割り当てを超過すると、スイッチはポートへの電力供給をオフにします (デフォルトのアクション)。
-------------------	---

デフォルト

受電装置のリアルタイムの電力消費のポリシングは、ディセーブルです。スイッチは、リアルタイムの電力消費をポリシングしません。

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	変更箇所
12.2(53)EX	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、Power of Ethernet (PoE) 対応ポートのみ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。

power inline police [action log] コマンドは、PoE ポートを備えたスイッチのみでサポートされています。

リアルタイムの電力消費のポリシングがイネーブルである場合、受電装置が割り当てられた最大電力より多くの量を消費すると、スイッチが対処します。

PoE がイネーブルである場合、スイッチは受電装置のリアルタイムの電力消費を検知します。この機能は、**パワー モニタリング** または **パワー センシング** といわれます。また、スイッチは **パワー ポリシング** 機能を使用して消費電力をポリシングします。

電力ポリシングがイネーブルの場合、スイッチは次の順序でいずれかの値を PoE ポートでのカットオフ電力の値とします。

1. スイッチがポートに対して予定しているユーザ定義電力レベルを設定している場合は、**power inline consumption default wattage** グローバル コンフィギュレーション コマンドまたは **power inline consumption wattage** 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手動で行う。

2. ポートで許可されている電力を制限するユーザ定義電力レベルを設定している場合は、**power inline auto max max-wattage** または **power inline static max max-wattage** 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手動で行う。
3. スイッチにおいてデバイスの電力消費が設定されている場合は、CDP 電力ネゴシエーションまたは IEEE 分類を使用して自動的に行われる。
4. スイッチにおいて電力消費がデフォルト値の 15.4 W に設定されている場合は自動的に行われる。

power inline consumption default wattage グローバル コンフィギュレーション コマンド、**power inline consumption wattage** インターフェイス コンフィギュレーション コマンド、または **power inline [auto | static max] max-wattage** コマンドを入力して、カットオフ電力値を手動で設定するには、上記リストの 1 番めおよび 2 番めの方式を使用します。カットオフ電力値を手動で設定しない場合、スイッチは CDP 電力ネゴシエーションまたは受電装置の IEEE 分類を使用して、自動的に値を求めます。これは前述のリストの 3 番めの方法です。スイッチがこれらのいずれかの方法によっても値を求めることができない場合、スイッチはデフォルト値の 15.4 W（前述のリストの 4 番めの方法）を使用します。



(注)

カットオフ電力値、スイッチが使用する電力消費値、および接続装置の実際の電力消費値については、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」の章の「Power Monitoring and Power Policing」の項を参照してください。

パワー ポリシングがイネーブルである場合、スイッチはリアルタイムの電力消費を PoE ポートに割り当てられた最大電力と比較して、消費電力をポリシングします。装置が最大電力割り当て（またはカットオフ電力）を超える電力をポートで使用している場合、スイッチでは、ポートへの電力供給がオフにされるか、または装置に電力を供給しながら Syslog メッセージが生成されて LED（ポート LED はオレンジ色に点滅）が更新されます。

- ポートへの電力供給をオフにして、ポートを **errdisable** ステートとするようスイッチを設定するには、**power inline police** 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。
- 装置に電力を供給しながら、Syslog メッセージを生成するようスイッチを設定するには、**power inline police action log** コマンドを使用します。

action log キーワードを入力しない場合のデフォルトのアクションは、ポートのシャットダウン、ポートへの電力供給のオフ、およびポートを PoE **errdisable** ステートに移行、になります。PoE ポートを **errdisable** ステートから自動的に回復するよう設定するには、**errdisable detect cause inline-power** 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、PoE 原因に対する **errdisable** 検出をイネーブルにして、**errdisable recovery cause inline-power interval interval** グローバル コンフィギュレーション コマンドを使用して、PoE **errdisable** 原因の回復タイマーをイネーブルにします。



注意

ポリシングがディセーブルである場合、受電装置がポートに割り当てられた最大電力より多くの量を消費しても対処されないため、スイッチに悪影響を与える場合があります。

例

次の例では、電力消費のポリシングをイネーブルにして、スイッチの PoE ポートで Syslog メッセージを生成するようスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline police action log
```

設定を確認するには、**show power inline police** 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 inline-power	PoE 原因に対する errdisable 検出をイネーブルにします。
errdisable recovery cause inline-power	PoE 回復メカニズム変数を設定します。
power inline	PoE ポート上で電力管理モードを設定します。
power inline consumption	IEEE 分類によって受電装置に指定された電力量を上書きします。
show power inline police	リアルタイムの電力消費に関するパワー ポリシング情報を表示します。

priority

出力ポリシー マップに属するトラフィックのクラスに対してクラスベース プライオリティ キューイングを設定するには、**priority** 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。スイッチでは、完全プライオリティ キューイングまたは **police** ポリシーマップ コマンドと併用されるプライオリティをサポートしています。クラスに指定されているプライオリティを削除するには、このコマンドの **no** 形式を使用します。

priority

no priority



(注)

priority ポリシーマップ クラス コマンドで **police** コマンドを使用してプライオリティ キューを無条件にレート制限すると、**police** コマンドでバースト サイズの値はサポートされません。

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

単独で使用されている場合 (**police** ポリシーマップ コマンドの前ではなく)、**priority** コマンドは低遅延パスにトラフィックを割り当て、クラスに属するパケットの遅延が設定可能な最小遅延になるようにします。完全プライオリティ キューイングを使用すると、プライオリティ キューのパケットはキューが空になるまでスケジューリングされ、送信されます。



(注)

policy コマンドなしで **priority** コマンドを使用する際は注意してください。完全プライオリティ キューイングを過剰に使用すると、他のキューで輻輳が発生する場合があります。

プライオリティ キューで使用される帯域幅を削減するには、**priority** を **police {rate-bps | cir cir-bps}** ポリシーマップ コマンドと併用します。これは、出力ポリシー マップでサポートされる唯一のポリシー形式です。このようにコマンドを組み合わせると、プライオリティ キューの最大レートを設定します。また、他のクラスに **bandwidth** および **shape average** の各ポリシーマップ コマンドを使用すると、他のキューのトラフィック レートを割り当てることができます。



(注)

出力ポリシーで **police** コマンドと **priority** コマンドを併用する場合に、コマンドライン ヘルプで表示される範囲が 8000 ~ 1000000000 bps であっても、ポリシング レートの範囲は 64000 ~ 1000000000 bps です。出力サービス ポリシーを付加しようとする、設定済みのバースト サイズは無視されます。

出力ポリシー マップに **police** コマンドを使用せずにプライオリティを設定する場合に他のキューを設定するには、**bandwidth remaining percent** ポリシーマップ コマンドを使用して、共有するしかありません。このコマンドは、割り当てられた帯域幅を保証しませんが、分散レートは保証されます。

出力ポリシー マップに **police** コマンドを使用してプライオリティを設定する場合に他のキューを設定するには、**bandwidth** ポリシーマップ コマンドを使用して共有し、**shape average** ポリシーマップ クラス コマンドを使用してシェーピングするしかありません。

priority コマンドは、スイッチ上で付加されたすべての出力ポリシーの単一の一意のクラスにのみ関連付けられます。

priority コマンドは、出力ポリシー マップの **class-default** に関連付けられません。

同一クラスでは、プライオリティとその他のスケジューリング アクション (**shape average** または **bandwidth**) を設定できません。

priority コマンドは、クラスのデフォルト キュー制限を使用します。キュー制限を変更するには、**queue-limit** ポリシーマップ クラス コマンドを使用し、**priority** コマンドによって設定されたデフォルト設定を上書きします。

例

次に、クラス *out-class1* を完全プライオリティ キューとして設定し、このクラスのすべてのパケットが他のトラフィック クラスより先に送信される例を示します。他のトラフィック キューでは、*out-class2* は残りの帯域幅の 50%、*out-class3* は残りの帯域幅の 20% を取得するように設定されます。クラス **class-default** は、保証なしで、残りの 30% を取得します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

次に、**priority** コマンドと **police** コマンドを併用して、*out-class1* をプライオリティ キューとして設定し、キューに着信するトラフィックを 20000000 ビット/秒 (bps) に制限して、プライオリティ キューがそれを超えるレートを使用しないようにする例を示します。このレートを超えるトラフィックは、廃棄されます。その他のトラフィック キューは、前述の例のとおり設定されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# 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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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	Quality of Service (QoS) ポリシー マップを表示します。

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	変更箇所
12.2(53)EX	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 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ド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 として設定できます。

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。コミュニティ VLAN には、最大 8 つのユーザ ネットワーク インターフェイス (UNI) を含めることができます。

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 は、リモート スイッチド ポート アナライザ (RSPAN) VLAN にすることはできません。

プライベート VLAN は、User Network Interface-Enhanced Network Interface (UNI-ENI) にすることはできません。VLAN が UNI-ENI 隔離 VLAN (デフォルト) の場合、**private-vlan VLAN** コンフィギュレーション コマンドを入力して、プライベート VLAN に変更できます。VLAN が UNI-ENI コミュニティ VLAN として設定されている場合、最初に **no uni-vlan VLAN** コンフィギュレーション コマンドを入力してから、プライベート VLAN として設定する必要があります。

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の詳細については、**switchport private-vlan** コマンドを参照してください。



(注)

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。この例では、VLAN 502 および VLAN 503 は、事前に UNI-ENI コミュニティ VLAN として設定されていると想定します。

```
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)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no uni-vlan
```

```
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 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 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。インターフェイスからプライベート 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

<i>secondary-vlan-list</i>	プライマリ VLAN インターフェイス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 インターフェイス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 インターフェイス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 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	変更箇所
12.2(53)EX	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 のインターフェイス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 VLAN 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	インターフェイスまたは 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-limit

出力ポリシー マップの重み付きテールドロップ (WTD) のキューの最大しきい値を設定するには、**queue-limit** 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。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。

```
queue-limit [cos value | dscp value | precedence value | qos-group value]
             number-of-packets [packets]
```

```
no queue-limit [cos value | dscp value | precedence value | qos-group value]
                number-of-packets [packets]
```

構文の説明

cos value	(任意) 各サービス コスト (CoS) 値のパラメータを設定します。指定できる範囲は 0 ~ 7 です。
dscp value	(任意) 各 DiffServ コード ポイント (DSCP) 値のパラメータを設定します。指定できる範囲は 0 ~ 63 です。
precedence value	(任意) 各 IP precedence 値のパラメータを設定します。指定できる範囲は 0 ~ 7 です。
qos-group value	(任意) 各 Quality Of Service (QoS) グループ値のパラメータを設定します。指定できる範囲は 0 ~ 99 です。
number-of-packets [packets]	キューの packets 数として WTD の最大しきい値を設定します。指定できる範囲は 16 ~ 544 で、256 バイトの packets を表します。デフォルトは 160 packets です。 packets キーワードは任意です。 (注) 最適なネットワーク パフォーマンスを得るには、最大キュー制限を 272 以下に設定することを強く推奨します。

デフォルト

デフォルトのキュー制限は 160 (256 バイト) packets 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

出力トラフィックを制御するには、**queue-limit** ポリシーマップ クラス コマンドを使用します。キュー制限設定は、入力ポリシー マップでサポートされません。

Cisco IOS Release 12.2(35)SE 以降では、インターフェイスごとに 1 つの出力ポリシー マップがサポートされます。ただし、すべての出力ポリシー マップにおいて 3 つの固有のキュー制限設定は有効なままとなります。複数のポリシー マップで同じキュー制限設定を使用できます。

出力ポリシー マップ内で許容されるキュー (クラス) は 4 つだけです (クラス デフォルトを含む)。各キューには 3 つのしきい値が定義されています (キュー制限)。スイッチに許可されるのは 3 つのキュー制限設定のみですが、複数のポリシー マップで同じキュー制限を共有できます。2 つのポリシー マップがキュー制限の設定を共有する場合、両方のポリシー マップのすべてのクラスで、すべてのしきい値が同じでなければなりません。

4 つ目のキュー制限設定を含む出力ポリシー マップをインターフェイスに付加しようとする、エラーメッセージが表示され、付加は許可されません。

queue-limit コマンドは、出力ポリシー マップの **class-default** で **queue-limit** を設定している場合を除き、**bandwidth**、**shape-average**、または **priority** などのスケジューリング アクションを最初に設定した後にのみサポートされます。

queue-limit コマンドで、WTD 修飾子 (**cos**、**dscp**、**precedence**、**qos-group**) に 3 つ以上の一意的しきい値を設定できません。ただし、これらのしきい値には、任意の数の修飾子をマッピングできます。修飾子なしの **queue-limit** コマンドを使用することにより、3 番目の一意的しきい値を設定して、最大キューを設定できます。

queue-limit コマンドを使用して、クラス マップ内のしきい値を設定する場合、WTD しきい値は、キューの最大しきい値以下にする必要があります。これは、修飾子なしで設定されたキュー サイズが修飾子で設定されているキュー サイズ大きい修飾子に設定されているいずれのキュー サイズよりも大きい必要があることを意味します。

例

次に、*out-class1*、*out-class2*、*out-class3*、および **class-default** がそれぞれ最低 40、20、10、および 10% のトラフィック帯域幅を取得するように、WTD を設定する例を示します。対応するキューサイズは、48、32、16、および 272 (256 バイト) パケットに設定されます。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# queue-limit 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 272
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

次に、*outclass1*、*outclass2*、および *outclass3* がそれぞれ最低 50、20、および 10% のトラフィック帯域幅を取得するようにファストイーサネットポートの WTD を設定する例を示します。**class-default** は、残りの 20% を得します。対応する各キューサイズは、64、32、および 16 (256 バイト) パケットに設定されます。また、この例では、*outclass1* が dscp 46、56、57、58、60、63 に一致する場合、DSCP 値 46 が 32 (256 バイト) パケットのキューサイズ、DSCP 値 56、57、および 58 が 48 (256 バイト) パケット、残りの DSCP 値 60 および 63 はデフォルトキューサイズの 64 (256 バイト) パケットを取得することを示します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 64
Switch(config-pmap-c)# queue-limit dscp 46 32
Switch(config-pmap-c)# queue-limit dscp 56 48
Switch(config-pmap-c)# queue-limit dscp 57 48
Switch(config-pmap-c)# queue-limit dscp 58 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

スイッチ上の複数の出力ポリシー マップで同じキュー制限値を使用できます。ただし、クラスのキュー制限値の 1 つを変更すると、新たな固有のキュー制限設定が作成されます。インターフェイスに付加できる出力ポリシー マップの固有のキュー制限設定は、どの時点でも 3 つだけです。4 つ目のキュー制限が設定された出力ポリシー マップを付加しようとする、次のエラーメッセージが表示されます。

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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。

radius-server dead-criteria

RADIUS サーバが使用不可または デット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	変更箇所
12.2(53)EX	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
authentication event	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 <i>retries</i>	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。構文情報については、『 Cisco IOS Security Command Reference, Release 12.2 』>「 Server Security Protocols 」>「 RADIUS Commands 」を選択してください。
radius-server timeout <i>seconds</i>	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。構文情報については、『 Cisco IOS Security Command Reference, Release 12.2 』>「 Server Security Protocols 」>「 RADIUS Commands 」を選択してください。
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。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。

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

<i>ip-address</i>	RADIUS サーバの IP アドレスを指定します。
acct-port <i>udp-port</i>	(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 <i>udp-port</i>	(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 <i>name</i>	(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 <i>time</i>	(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 <i>string</i>	(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キーおよび暗号キーを指定します。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 を引用符で囲まなくてください。

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せん。

認証キーおよび暗号キー (*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	変更箇所
12.2(53)EX	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キーおよび暗号キーを設定できます。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tring 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
authentication event	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 デモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。構文情報については、『 Cisco IOS Security Command Reference, Release 12.2 』> 「 Server Security Protocols 」> 「 RADIUS Commands 」を選択してください。
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。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。

reload

オペレーティング システムをリロードするには、**reload** 特権 EXEC コマンドを使用します。

reload [**warm**] [**in** [*hh:mm*] | **at** *hh:mm* [*month day* | *day month*]] [**cancel**] [*text*]

構文の説明

warm	(任意) ストレージからイメージを読み取らずにスイッチをリロードします。スイッチのリブート時間が大幅に短縮され、システム全体の可用性が高まります。
in [<i>hh:mm</i>]	(任意) 指定した分数、または時間および分数が経過したときにソフトウェアがリロードされるようにスケジューリングします。リロードは、約 24 日以内に行う必要があります。
at <i>hh:mm</i>	(任意) ソフトウェアのリロードが (24 時間制で) 指定された時刻に行われるようにスケジューリングします。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます (指定時刻が現時刻より後の場合)。または翌日の指定時刻に行われます (指定時刻が現時刻よりも前の場合)。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、約 24 日以内に行う必要があります。
<i>month</i>	(任意) 月の名前。任意の文字数からなる一意のストリングです。
<i>day</i>	(任意) 1 ~ 31 の範囲で日付を指定します。
cancel	(任意) スケジューリングされているリロードをキャンセルします。
<i>text</i>	(任意) リロードの理由 (1 ~ 255 文字)。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

reload コマンドはシステムを停止させます。エラー発生時に再起動するようにシステムが設定されている場合は、自動的に再起動します。**reload** コマンドは、コンフィギュレーション情報がファイルに入力され、スタートアップ コンフィギュレーションに保存された後で使用します。

システムが自動ブートに設定されていない仮想端末からはリロードできません。これは、システムが ROM モニタにドロップし、リモート ユーザの制御からシステムを削除することを防止するためです。

コンフィギュレーション ファイルを変更すると、コンフィギュレーションを保存するように指示するプロンプトが表示されます。存在しないスタートアップ コンフィギュレーション ファイルを変数 CONFIG_FILE が示している場合は、保存動作中に、保存を進めるかどうかの確認が要求されます。この状況で [Yes] と応答すると、リロード時にセットアップ モードが開始されます。

後でリロードを実行するようにスケジュールする場合は、約 24 日以内にリロードを実行する必要がある場合があります。

at キーワードを使用できるのは、ルータでシステム クロックが (NTP、ハードウェア カレンダー、または手動で) 設定されている場合だけです。この時間は、ルータの設定された時間帯と相対的です。複数のルータで同時にリロードが行われるように設定する場合は、各ルータの時刻を NTP によって同期させる必要があります。

ストレージからイメージを読み取らずにスイッチをリロードするには、**warm** キーワードを使用します。Cisco IOS イメージは、ROM モニタ モード (ROMMON) の介入なしでリブートします。これにより、以前 RAM に保存されたコピーから読み取り / 書き込みデータが復元され、イメージのフラッシュ メモリから RAM へのコピーやイメージの自己解凍なしで実行が開始されます。したがって、スイッチはより高速でリブートします。

warm キーワードを使用すると、手動で起動するように設定しても、スイッチは自動的に起動します。スケジューリングされたリロードの情報を表示するには、**show reload EXEC** コマンドを使用します。

例

次に、ただちにスイッチのソフトウェアをリロードする例を示します。

```
Switch# reload
```

次の例では、スイッチのソフトウェアは 10 分以内にリロードされます。

```
Switch# reload in 10
```

```
Switch# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reload?[confirm]
Switch#
```

次の例では、スイッチのソフトウェアは本日 13:00 にリロードされます。

```
Switch# reload at 13:00
```

```
Switch# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload?[confirm]
Switch#
```

次の例では、スイッチのソフトウェアは 4 月 20 日の 2:00 にリロードされます。

```
Switch# reload at 02:00 apr 20
```

```
Switch# Reload scheduled for 02:00:00 PDT Sat Apr 20 1996 (in 38 hours and 9 minutes)
Proceed with reload?[confirm]
Switch#
```

次に、保留中のリロードを取り消す例を示します。

```
Switch# reload cancel
```

```
%Reload cancelled.
```

次の例では、本日 4:00 にウォーム リブートを実行します。

```
Switch# reload warm at 4:00
```

関連コマンド

コマンド	説明
copy system:running-config nvram:startup-config	コピー元からコピー先に任意のファイルをコピーします。
show reload	ルータのリロード ステータスを表示します。

remote-span

VLAN を Remote Switched Port Analyzer (RSPAN; リモート スイッチド ポート アナライザ) 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

有効な RSPAN VLAN ID は 2 ~ 1001 および 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。

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。

- VLAN を User Network Interface-Enhanced Network Interface (UNI-ENI) 隔離 VLAN (デフォルト) から RSPAN VLAN に変更するには、**rspan-vlan** VLAN コンフィギュレーション コマンドを入力します。
- UNI-ENI コミュニティ VLAN を RSPAN VLAN に変更するには、**no uni-vlan** VLAN コンフィギュレーション モード コマンドを入力してまずコミュニティ VLAN を削除する必要があります。

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; スパニング ツリー プロトコル) は RSPAN VLAN 内では稼働できませんが、RSPAN 宛先ポートでは稼働しません。Cisco CGS 2520 スイッチでは、STP がイネーブルにされているネットワーク ノード インターフェイス (NNI) と拡張ネットワーク インターフェイス (ENI) だけが STP に参加します。

また、RSPAN VLAN ID を使用して、手動で送信元スイッチ、宛先スイッチ、および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)。

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; スイッチド ポート アナライザ) 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。
vlan	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

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 [validation none] [{flash:/filename |
ftp://user:password@host/filename | nvram:/filename | rcp://user@host/filename |
tftp://host/filename}] [validation none]
```

構文の説明

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。
flash:/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。
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 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 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 Copy Protocol (RCP; リモート コピー プロトコル) 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 サーバにあることを指定します。

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	変更箇所
12.2(53)EX	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、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

■ renew ip dhcp snooping database

コマンド	説明
<code>ip dhcp snooping</code>	VLAN 上で DHCP スヌーピングをイネーブルにします。
<code>ip dhcp snooping binding</code>	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。
<code>show ip dhcp snooping database</code>	DHCP スヌーピング データベース エージェントのステータスを表示します。

rep admin vlan

Resilient Ethernet Protocol (REP; レジリエントイーサネットプロトコル) が Hardware Flood Layer (HFL; ハードウェアフラッドレイヤ) メッセージを送信するように REP 管理 VLAN を設定するには、**rep admin 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 (VLAN 1 が管理 VLAN) に戻す場合は、このコマンドの **no** 形式を使用します。

rep admin vlan *vlan-id*

no rep admin vlan

構文の説明	<i>vlan-id</i>	VLAN ID の範囲は 1 ~ 4094 です。デフォルトは VLAN 1 のため、設定する範囲は 2 ~ 4094 です。
--------------	----------------	---

デフォルト 管理 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	変更箇所
	12.2(53)EX	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 がまだ存在していない場合、このコマンドにより VLAN が作成されることはありません。ロード バランシング時のリンク障害や VLAN ブロッキングの通知のメッセージをソフトウェアでリレーすることによって発生する遅延を回避するために、REP は HFL で通常のマルチキャストアドレスにパケットをフラディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラディングされます。セグメントに属していないスイッチは、これらのメッセージをデータトラフィックとして扱います。ドメイン全体の管理 VLAN を設定することにより、これらのメッセージのフラディングを管理できます。

REP 管理 VLAN が設定されていない場合、デフォルトは VLAN 1 になります。

スイッチとセグメントで 1 つの管理 VLAN だけが可能です。

管理 VLAN は RSPAN VLAN になりません。

例 次の例では、VLAN 100 を REP 管理 VLAN として設定する方法を示します。

```
Switch (config)# rep admin vlan 100
```

設定を確認するには、**show interface rep 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
	show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep block port

Resilient Ethernet Protocol (REP) VLAN ロード バランシングを設定するには、REP プライマリ エッジポートで **rep block 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。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。

```
rep block port {id port-id | neighbor_offset | preferred} vlan {vlan-list | all}
```

```
no rep block port {id port-id | neighbor_offset | preferred}
```

構文の説明

id port-id	REP イネーブル時に自動的に生成される一意のポート ID を入力することで、VLAN ブロック代替ポートを識別します。REP ポート ID は、16 文字の 16 進数値です。インターフェイスのポート ID を表示するには、 show interface interface-id rep detail コマンドを入力します。
neighbor_offset	ネイバーのオフセット番号を入力することで、VLAN ブロック代替ポートを識別します。指定できる範囲は -256 ~ +256 で、値 0 は無効です。プライマリ エッジポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジポートのダウンストリーム ネイバーを識別します。負の番号は、セカンダリ エッジポート (オフセット番号 -1) とダウンストリーム ネイバーを識別します。
preferred	VLAN ブロック代替ポートを、 rep segment segment-id preferred 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セグメントポートとして識別します。 (注) preferred キーワードを入力しても確実に代替ポートは指定されませんが、他の類似のポートより優先されます。
vlan	ブロックする VLAN を識別します。
vlan-list	ブロックする VLAN について、1 ~ 4094 の範囲の VLAN ID を入力するか、VLAN ID の範囲または連続番号 (1-3、22、41-44 など) を入力します。
all	すべての VLAN をブロックするように入力します。

デフォルト

rep preempt segment 特権 EXEC コマンド (手動プリエンブション) を入力した場合のデフォルトのアクションは、プライマリ エッジポートで VLAN すべてがブロックされます。この動作は **rep block port** コマンドを設定するまで継続されます。

プライマリ エッジポートで代替ポートを判別できない場合は、デフォルトのアクションはプリエンブションなし、および VLAN ロード バランシングなしです。

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

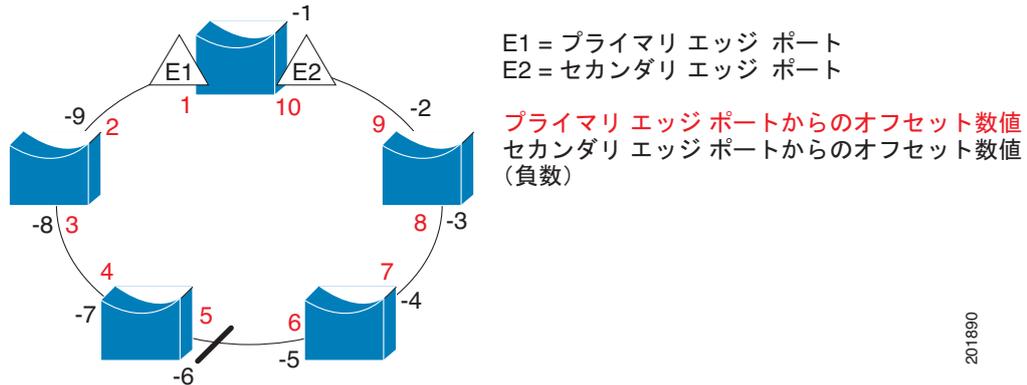
リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、REP プライマリ エッジ ポート上に入力する必要があります。

オフセット番号を入力して代替ポートを選択する場合、オフセット番号はエッジポートのダウンストリーム ネイバー ポートを識別します。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負の番号は、セカンダリ エッジ ポート (オフセット番号 -1) とダウンストリーム ネイバーを識別します。「REP セグメントのネイバー オフセット番号」図 2-1 を参照してください。

図 2-1 REP セグメントのネイバー オフセット番号



201800



(注)

番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

rep preempt delay seconds 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でプリエンプレッション遅延時間を設定して、リンク障害とリカバリが発生した場合、別のリンク障害が発生することなく設定したプリエンプレッション期間が経過すると、VLAN ロード バランシングが開始されます。ロードバランシング設定で指定された代替ポートは、設定された VLAN をブロックし、その他すべてのセグメント ポートのブロックを解除します。プライマリ エッジ ポートで VLAN バランシングの代替ポートを決定できない場合、デフォルトのアクションはプリエンプレッションなしになります。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID の形式は、スパンニング ツリー アルゴリズムで使用されるものと同様で、MAC アドレス (ネットワーク内で一意) に関連付けられるポート番号 (ブリッジ上で一意) となります。ポートのポート ID を判別するには、**show interface interface-id rep detail** 特権 EXEC コマンドを入力します。

例

次の例では、スイッチ B プライマリ エッジ ポート (ギガビット イーサネット ポート 0/1) の REP VLAN ロード バランシングを設定して、スイッチ A のギガビット イーサネット ポート 0/2 を代替ポートとして設定して VLAN 1 ~ 100 をブロックする方法を示します。代替ポートは、スイッチ A ポートの **show interface rep detail** コマンドの出力に太字で表示されるポート ID により識別されます。

```
Switch A# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
```

rep block port

```
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493
```

```
Switch B# config t
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Switch (config-if)# exit
```

次の例では、ネイバー オフセット番号を使用して VLAN ロード バランシングを設定する方法と、**show interfaces rep detail** 特権 EXEC コマンドを入力して設定を確認する方法について示します。

```
Switch# config t
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep block port 6 vlan 1-110
Switch (config-if)# end

Switch# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

関連コマンド

コマンド	説明
rep preempt delay	ポート障害とリカバリの後から REP VLAN ロード バランシングがトリガーされるまでの待機期間を設定します。
rep preempt segment	手動でセグメント上の REP VLAN ロード バランシングを開始します。
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの REP 詳細設定およびステータスを表示します。

rep lsl-age-timer

REP インターフェイスが REP ネイバーから hello を受信せずに起動し続ける時間の Link Status Layer (LSL) エージング タイマーを設定するには、Resilient Ethernet Protocol (REP) ポートで **rep lsl-age-timer** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト時間に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-age timer value

no rep lsl-age timer

構文の説明

<i>value</i>	エージアウト時間 (ミリ秒)。指定できる範囲は 120 ~ 10000 ミリ秒 (40 ミリ秒単位) です。デフォルト値は 5000 ミリ秒 (5 秒) です。
--------------	--

デフォルト

REP リンクは、5000 ミリ秒間ネイバーから hello メッセージを受信しなければ、シャットダウンされます。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

LSL エージング タイマーの間に少なくとも 2 つの LSL hello が送信されるように、LSL Hello タイマーはエージング タイマーの値を 3 で割った値に設定されます。この期間に hello が受信されない場合、REP リンクはシャットダウンします。

Cisco IOS Release 12.2(52)SE では、LSL エージング タイマーの範囲が 3000 ~ 10000 ミリ秒 (500 ミリ秒単位) から 120 ~ 10000 ミリ秒 (40 ミリ秒単位) に変更されています。REP ネイバー デバイスで Cisco IOS Release 12.2(52)SE 以降が稼動していない場合、デバイスは以前の範囲を逸脱する値を受け付けないため、時間の範囲を短くする必要があります。

EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとする、エラーメッセージが表示されてコマンドが拒否されます。

例

次の例では、REP リンクの REP LSL エージング タイマーを 7000 ms に設定する方法を示します。

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep lsl-age-timer 7000
Switch (config-if)# exit
```

設定されたエージアウト時間を確認するには、**show interfaces rep detail** 特権 EXEC コマンドを入力します。

■ rep lsl-age-timer

関連コマンド

コマンド	説明
show interfaces rep [detail]	設定済みの LSL エージアウト タイマー値を含め、すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

rep preempt delay

セグメントポートの障害および回復の発生後 Resilient Ethernet Protocol (REP) VLAN ロード バランシングがトリガーされるまでの待機時間を設定するには、REP プライマリ エッジポートで **rep preempt delay** 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。設定された遅延を削除するには、このコマンドの **no** 形式を使用します。

rep preempt delay seconds

no rep preempt delay

構文の説明

<i>seconds</i>	REP プリエンプションを遅延させる秒数を設定します。指定できる範囲は 15 ～ 300 です。
----------------	--

デフォルト

プリエンプション遅延は設定されていません。**rep preempt delay** コマンドを入力しない場合、デフォルトは遅延のない手動プリエンプションとなります。

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	変更箇所
12.2(53)EX	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、REP プライマリ エッジポート上に入力する必要があります。

リンク障害とリカバリ後に自動的に VLAN ロード バランシングをトリガーする場合、このコマンドを入力してプリエンプション時間遅延を設定する必要があります。

VLAN ロード バランシングが設定されている場合、セグメントポート障害とリカバリの後、VLAN ロード バランシングが発生する前に REP プライマリ エッジポートで遅延タイマーが起動されます。各リンク障害が発生した後にタイマーが再起動することに注意してください。タイマーが満了となると、(**rep block 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設定された) VLAN ロード バランシングを実行するように REP プライマリ エッジが代替ポートに通知し、新規トポロジ用のセグメントが準備されます。設定された VLAN リストは代替ポートでブロックされ、他のすべての VLAN はプライマリ エッジポートでブロックされます。

例

次の例では、プライマリ エッジポートで REP プリエンプション時間遅延を 100 秒に設定する方法を示します。

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep preempt delay 100
Switch (config-if)# exit
```

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

■ rep preempt delay

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep	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 REP 設定およびステータスを表示します。

rep preempt segment

セグメントで Resilient Ethernet Protocol (REP) VLAN ロード バランシングを手動で開始するには、**rep preempt segment** 特権 EXEC コマンドを使用します。

rep preempt segment *segment_id*

構文の説明

segment-id REP セグメントの ID。指定できる範囲は 1 ~ 1024 です。

デフォルト

デフォルト動作は手動プリエンブションです。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

rep preempt segment *segment-id* コマンドを入力すると、プリエンブションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

プライマリ エッジ ポートのあるセグメントのスイッチにこのコマンドを入力します。

VLAN ロード バランシングを設定しない場合、このコマンドを入力するとデフォルトの動作になります (プライマリ エッジ ポートですべての VLAN がブロックされます)。

手動でプリエンブションを開始する前に、REP プライマリ エッジ ポートで **rep block port {id port-id | neighbor_offset | preferred} vlan {vlan-list | all}** 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、VLAN ロード バランシングを設定します。

このコマンドには、**no** バージョンはありません。

例

次の例では、確認メッセージ付きで、セグメント 100 で REP プリエンブションを手動でトリガーする方法を示します。

```
Switch)# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep [detail]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

rep segment

インターフェイスで Resilient Ethernet Protocol (REP) をイネーブルにして、セグメント ID を割り当てるには、**rep segment** 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 REP 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。

rep segment segment-id [edge [no-neighbor] [primary]] [preferred]

no rep segment

構文の説明

<i>segment-id</i>	セグメント ID をインターフェイスに割り当てます。指定できる範囲は 1 ~ 1024 です。
edge	(任意) 2 つの REP エッジ ポートの 1 つとしてインターフェイスを識別します。 primary キーワードなしで edge キーワードを入力すると、ポートがセカンダリ エッジ ポートとして設定されます。
primary	(任意) エッジ ポートで、ポートがプライマリ エッジ ポートであると指定します。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。
preferred	(任意) ポートを優先代替ポートまたは VLAN ロード バランシングの優先ポートに指定します。 (注) ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。

デフォルト

REP はインターフェイスでディセーブルです。

REP がインターフェイスでイネーブルの場合、デフォルトでは通常のセグメント ポートであるポートに対して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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

REP ポートは、レイヤ 2 トランク ポートである必要があります。

非 ES REP ポートは、IEEE 802.1Q トランク ポートまたは ISL トランク ポートのいずれかになります。

REP ポートは次のいずれかのポート タイプとして設定してはいけません。

- SPAN 宛先ポート
- プライベート VLAN ポート
- トンネル ポート

- アクセス ポート
- REP ポートは、ネットワーク ノード インターフェイス (NNI) である必要があります。ユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) を REP ポートにはできません。

各 REP セグメント上には、プライマリ エッジ ポートと、セカンダリ エッジ ポートとして機能するポートの、2 種類のエッジ ポートを設定しなければいけません。たとえば別のスイッチにあるポートなどの、セグメント内の 2 つのポートをプライマリ エッジ ポートとして指定すると (設定は可能です)、REP によりその内の 1 つがセグメントのプライマリ エッジ ポートとして機能するように選択されます。

- REP ポートは以下の規則に従います。
 - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
 - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。
 - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジ ポートであるか、両方のポートが通常セグメント ポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。
 - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメント ポートに設定されている場合 (設定ミス)、エッジ ポートは通常セグメント ポートとして扱われます。

別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。いずれのポートがプライマリ エッジ ポートかを確認するには、**show rep topology** 特権 EXEC コマンドをセグメント内のポートに入力します。

REP インターフェイスはブロック ステートで起動し、安全にブロック解除可能と通知されるまでブロック ステートのままになります。突然の接続切断を避けるために、これを意識しておく必要があります。

冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

ネイバー スイッチ上のポートで REP がサポートされていないネットワークでは、非 REP 側ポートを非ネイバー エッジ ポートとして設定できます。非ネイバー エッジ ポートはエッジ ポートのすべてのプロパティを継承するため、非ネイバー エッジ ポートをその他のいずれのエッジ ポートとしても設定できます。これには、STP または REP トポロジ変更通知をアグリゲーション スイッチに送信することも含まれます。この場合、送信される STP Topology Change Notification (TCN; トポロジ変更通知) は、Multiple Spanning-Tree (MST) STP メッセージです。

例 次の例では、通常の (非エッジ) セグメント ポートで REP をイネーブルにする方法を示します。

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep segment 100
```

次の例では、ポートの REP をイネーブルし、REP プライマリ エッジ ポートとして指定する方法を示します。

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep segment 100 edge primary
```

次に、インターフェイスに外部 REP ネイバーがない場合の同じ設定の例を示します。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 100 edge no-neighbor primary
```

次の例では、ポートの REP をイネーブルし、REP セカンダリ エッジ ポートとして指定する方法を示します。

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep segment 100 edge
```

設定を確認するには、**show interfaces rep** 特権 EXEC コマンドを入力します。セグメントのいずれのポートがプライマリ エッジ ポートであるか確認するには、**show rep topology** 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 rep [detail]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。
show rep topology [detail]	プライマリ エッジ ポートとして設定および選択されたポートを含む、セグメント内のすべてのポートに関する情報を表示します。

rep stcn

REP Segment Topology Change Notification (STCN; セグメント トポロジ変更通知) を他のインターフェイス、他のセグメントまたは Spanning Tree Protocol (STP) ネットワークに送信する設定を行うには、Resilient Ethernet Protocol (REP) エッジポートで **rep stcn** 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。STCN をインターフェイス、セグメント、または STP ネットワークに送信すること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。

```
rep stcn {interface interface-id | segment id-list | stp}
```

```
no rep stcn {interface | segment | stp}
```

構文の説明

interface interface-id	STCN を受信するように物理インターフェイスまたはポート チャネルを識別します。
segment id-list	STCN を受信する 1 REP セグメントまたはセグメントのリストを識別します。有効範囲は 1 ~ 1024 です。一連のセグメント (たとえば 3-5、77、100 など) を設定することもできます。
stp	STCN を STP ネットワークに送信します。

デフォルト

他のインターフェイス、セグメント、または STP ネットワークへの STCN の送信がディセーブルです。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このコマンドをセグメント エッジ ポートに入力します。

このコマンドを使用して、ローカル REP セグメントで発生しているトポロジ変更をレイヤ 2 ネットワークの他の部分に通知します。これにより、ネットワークの他部分にあるレイヤ 2 転送テーブル内の廃止エントリが削除され、より高速なネットワーク コンバージェンスが可能になります。

例

次の例では、REP プライマリ エッジ ポートでセグメント 25 ~ 50 に STCN を送信する設定方法を示します。

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep stcn segment 25-50
Switch (config-if)# exit
```

設定を確認するには、**show interfaces rep 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
<code>show interfaces rep [detail]</code>	すべてのインターフェイスまたは指定したインターフェイスの REP 設定および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	変更箇所
12.2(53)EX	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。

■ reserved-only

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	
<i>index</i>	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。
<i>owner name</i>	（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	変更箇所
	12.2(53)EX	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。ポートがユーザ ネットワーク インターフェイス（UNI）または拡張ネットワーク インターフェイス（ENI）の場合、**rmon collection stats** コマンドを使用する前に **no shutdown** インターフェイス コンフィギュレーション コマンドを使用してインターフェイスをイネーブルにする必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス（NNI）はデフォルトでイネーブルです。

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 gigabitethernet0/1
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。 構文情報については、『Cisco IOS Configuration Fundamentals Command Reference, Release 12.2』>「System Management Commands」>「RMON Commands」を選択してください。

scada modbus tcp server

スイッチで MODBUS TCP をイネーブルにし、スイッチを MODBUS TCP サーバとして使用するには、**scada modbus tcp 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。MODBUS をディセーブルにし、デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

scada modbus tcp server [**connection** *connection-requests* | **port** *tcp-port-number*]

no scada modbus tcp server [**connection** *connection-requests* | **port** *tcp-port-number*]

構文の説明

connection <i>connection-requests</i>	(任意) スイッチに送信される同時接続要求の数を設定します。 <i>connection-requests</i> に指定できる範囲は 1 ~ 5 です。デフォルトは 1 です。
port <i>tcp-port-number</i>	(任意) クライアントがメッセージを送信する TCP ポートを設定します。 <i>tcp-port-number</i> に指定できる範囲は 1 ~ 65535 です。デフォルトは 502 です。

デフォルト

スイッチは MODBUS TCP サーバとして設定されていません。
TCP スイッチ ポート番号は 502 です。
同時接続要求の数は 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	変更箇所
12.2(53)EX	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 scada modbus tcp server コマンドを使用すると、MODBUS サーバが停止し、すべての MODBUS 接続とポートの設定が削除されます。

例

次に、スイッチで MODBUS TCP をイネーブルにし、スイッチに送信可能な同時接続要求数を 4 に設定して、TCP ポートを 801 に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# scada modbus tcp server

WARNING: Starting Modbus TCP server is a security risk.
Please understand the security issues involved before
proceeding further.Do you still want to start the
server?[yes/no]: y
Switch(config)# scada modbus tcp server connection 4
Switch(config)# scada modbus tcp server port 801
Switch(config)# end
```

次の例は、**show scada modbus tcp server** コマンドの出力を示します。

```
Switch# show scada modbus tcp server
Summary: enabled, running, process id 142

Conn Stats: listening on port 801, 4 max simultaneous connections
             0 current client connections
             0 total accepted connections, 0 accept connection errors
             0 closed connections, 0 close connection errors

Send Stats: 0 tcp msgs sent, 0 tcp bytes sent, 0 tcp errors
            0 responses sent, 0 exceptions sent, 0 send errors

Recv Stats: 0 tcp msgs received, 0 tcp bytes received, 0 tcp errors
            0 requests received, 0 receive errors
```

関連コマンド

コマンド	説明
clear scada modbus tcp server statistics	MODBUS TCP サーバおよびクライアントの統計情報をクリアします。
show scada modbus tcp server [connections]	サーバ情報および統計情報を表示します。クライアント情報および統計情報を表示するには、 connection キーワードを使用します。

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。スイッチでメトロ IP アクセス イメージが実行されている場合は、テンプレートを使用してレイヤ 2 とレイヤ 3 の機能間のリソースのバランスを取ることも、ハードウェアでレイヤ 2 機能のみをサポートして最大限システムを利用することもできます。デュアル IPv4/IPv6 テンプレートを選択して、IPv6 転送をサポートすることもできます。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 {default | dual-ipv4-and-ipv6 {default | routing | vlan} | layer-2}
```

```
no sdm prefer
```



(注)

default および **dual-ipv4-and-ipv6** キーワードは、スイッチ上にメトロ IP アクセス イメージがインストールされている場合にのみ表示されます。

構文の説明

default	すべての機能に対してバランスをとります。
layer-2	ルーティングをサポートしないで、レイヤ 2 機能で最大限システム リソースを利用します。
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。 <ul style="list-style-type: none"> • 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。

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。

メトロ アクセス イメージが稼動しているスイッチでは、レイヤ 2 テンプレートだけがサポートされません。

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	変更箇所
12.2(53)EX	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。スイッチでのルーティングをイネーブルにしない場合は、デフォルトテンプレートを使用しないでください。バランス テンプレートを使用すると、レイヤ 2 機能において、デフォルトテンプレートでユニキャスト ルーティングに割り当てられたメモリを使用できません。

スイッチがパケットをルーティングする場合はレイヤ 2 テンプレートを使用しないでください。レイヤ 2 テンプレートでは、ルーティングはサポートされていません。そのため、ルーティングはすべてソフトウェアを介して実行されます。これにより、CPU は過負荷となり、ルーティング パフォーマンスは大幅に低下します。

デュアル IPv4/IPv6 テンプレートを選択する前に IPv6 機能の設定を試みると、警告メッセージが表示されます。

デュアル スタック テンプレートでは、各リソースで使用可能な TCAM 容量が少なくなります。IPv4 トラフィックだけを転送する場合は、デュアル スタック テンプレートを使用しないでください。

表 2-5 に、メトロ IP アクセス イメージを稼動しているスイッチに対して 2 つの IPv4 テンプレートがそれぞれサポートする各リソースの概数を示します。テンプレートの値は、8 つのルーテッド インターフェイスおよび約 1024 の VLAN に基づき、テンプレートの選択時に設定されるおおよそのハードウェア境界を表します。ハードウェア リソースのある部分がいっぱいの場合、処理のオーバーフローはすべて CPU に送られ、スイッチのパフォーマンスに重大な影響が出ます。

表 2-5 に、各デュアル テンプレートによって割り当てられる機能リソースの概数を示します。この各テンプレートについての概数は、8 つのルーテッド インターフェイスと約 1000 の VLAN を持つスイッチに基づいて計算されています。

例

表 2-5 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

リソース	IPv4 および IPv6 のデフォルト	IPv4 および IPv6 のルーティング	IPv4 および IPv6 の VLAN
ユニキャスト MAC アドレス	2 K	1.5 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
IPv4 ユニキャスト ルートの合計 :	3 K	2.75 K	0
• IPv4 ホストに直接接続	2 K	1.5 K	0
• 間接 IPv4 ルート	1 K	1.25 K	0
IPv6 マルチキャスト グループ	1 K	1 K	1 K
IPv6 ユニキャスト ルートの合計 :	3 K	2.75 K	0
• 直接接続された IPv6 アドレス	2 K	1.5 K	0
• 間接 IPv6 ユニキャスト ルート	1 K	1.25 K	0
IPv4 ポリシー ベース ルーティング ACE	0	0.25 K	0
IPv4 または MAC QoS ACE (合計)	0.75 K	0.75 K	0.75 K
IPv4 または MAC セキュリティの ACE (合計)	1 K	0.5 K	1 K
IPv6 ポリシー ベース ルーティング ACE ¹	0	0.25 K	0
IPv6 QoS ACE	0.5 K	0.5 K	0.5 K
IPv6 セキュリティの ACE	0.5 K	0.5 K	0.5 K

1. IPv6 ポリシーベース ルーティングはサポートされません。

次に、スイッチ上でレイヤ 2 テンプレートを設定する例を示します。

```
Switch(config)# sdm prefer layer-2
Switch(config)# exit
Switch# reload
```

次は、テンプレートをレイヤ 2 テンプレートに変更し、スイッチをリロードしなかった場合の出力表示の一例です。

```
Switch# show sdm prefer
The current template is "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:          5K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:           9K
  number of directly-connected IPv4 hosts: 5K
  number of indirect IPv4 routes:         4K
number of IPv4 policy based routing aces: 0.5K
number of IPv4/MAC qos aces:             0.5K
number of IPv4/MAC security aces:        1K
On next reload, template will be "layer-2" template.
```

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 instance

インターフェイス上でイーサネット サービス インスタンスを設定し、イーサネット サービス コンフィギュレーション モードを開始するには、**service instance** 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。サービス インスタンスを削除するには、このコマンドの **no** 形式を使用します。

service instance *id* ethernet [*evc-id*]

no service instance *id*

このコマンドは、スイッチでメトロ IP アクセス イメージまたはメトロ アクセス イメージが稼動している場合にのみ使用できます。

構文の説明

<i>id</i>	VLAN にマップが適用されないインターフェイス単位のサービス ID であるサービス インスタンス ID を定義します。指定できる範囲は 1 ~ 4294967295 です。
ethernet	イーサネット インスタンスとしてサービス インスタンスを識別します。
<i>evc-id</i>	(任意) Ethernet Virtual Connection (EVC; イーサネット仮想接続) をサービス インスタンスに接続します。

デフォルト

イーサネット サービス インスタンスは定義されません。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

service instance *id* ethernet コマンドを入力した後、スイッチはイーサネット サービス コンフィギュレーション モードになり、次のコンフィギュレーション コマンドが利用できるようになります。

- **default** : サービス インスタンスをデフォルト ステートに設定します。
- **ethernet lmi ce-vlan map** : イーサネット Local Management Interface (LMI; ローカル管理インターフェイス) パラメータを設定します。 [ethernet lmi ce-vlan map](#) コマンドを参照してください。
- **exit** : EVC 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** : コマンドを無効にするか、コマンドをデフォルト設定に戻します。

例

次の例では、イーサネット サービス インスタンスを定義し、EVC *test* 用のイーサネット サービス コンフィギュレーション モードを開始します。

```
Switch(config-if)# service instance 333 ethernet test
Switch(config-if-srv)#
```

■ service instance

関連コマンド

コマンド	説明
<code>show ethernet service instance</code>	設定されたイーサネット サービス インスタンスに関する情報を表示します。

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ブレーク キーを押してブート 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

The password-recovery mechanism is enabled.

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	変更箇所
12.2(53)EX	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。これにより、認証および許可されたユーザに限定してコンフィギュレーション ファイルにアクセスできるようにしたコンフィギュレーション ファイル セキュリティ機能が提供され、ユーザがパスワード回復プロセスを使用してコンフィギュレーション ファイルにアクセスするのを防止できます。

パスワード回復手順では、ブレーク キーを使用する必要があります。スイッチが電源投入時自己診断テスト (POST) の実行後、自動起動プロセスを開始します。ブート ロードは、ブートアップ シーケンス中にユーザにブレーク キーの文字を求めるプロンプトを表示します (次の例を参照)。

```
***** The system will autoboot in 5 seconds *****
```

```
Send a break key to prevent autobooting.
```

システムが自動ブートを行うというメッセージを受信してから 5 秒以内にコンソール ターミナルにブレーク キーを入力する必要があります。スイッチに物理的にアクセスできるユーザは、フラッシュ メモリが初期化中のメッセージを受信してから 5 秒以内にコンソール ターミナルでブレーク キーを押します。システム LED は、**ブレーク キー**を受け入れるまでグリーンで点滅します。システム LED は、**ブレーク キー**を受け入れると、スイッチがブートされるまで消灯します。

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)?

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、**ブレーク キー**を押さないときと同じように通常のブート プロセスが続行します。システムをデフォルト値に戻すように設定すると、フラッシュ メモリ内のコンフィギュレーション ファイルが削除され、VLAN データベース ファイル `flash:vlan.dat` が存在する場合は、そのファイルも削除されます。



(注)

no service password-recovery コマンドを使用してパスワードへのエンド ユーザのアクセスを制御する場合は、エンド ユーザがパスワード回復手順を実行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コンフィギュレーション ファイルのコピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。

パスワード回復がイネーブルかディセーブルかを判別するには **show version** 特権 EXEC コマンドを入力できます。

例

次の例では、スイッチ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が得られた場合のみ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 (インターフェイス コンフィギュレーション)

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の着信または発信トラフィックに適用するには、**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 | output} policy-map-name
```

```
no service-policy {input | output} policy-map-name
```

構文の説明

input	物理ポートの入力に、ポリシーマップを適用します。
output	物理ポートの出力にポリシーマップを適用します。
<i>policy-map-name</i>	適用される指定のポリシーマップ。



(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。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

1つのインターフェイスに適用できるのは、1つの入力ポリシーマップと1つの出力ポリシーマップだけです。

Cisco IOS Release 12.2(35) SE からは、スイッチ上の各インターフェイスに出力ポリシーマップを適用できます。ただし、スイッチは、すべての出力ポリシーマップにおいて、同時に最大3個の固有のキュー制限設定のみがサポートされます。複数のポリシーマップで、同じキュー制限設定を共有できます。4つめのキュー制限が設定された出力ポリシーマップを適用しようとする、次のエラーメッセージが表示されます。

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit configurations exceeded.
```

ファストイーサネットまたはギガビットイーサネットポートに入力または出力ポリシーマップを適用できます。スイッチ仮想インターフェイス (SVI) および EtherChannel インターフェイスには、ポリシーマップを適用できません。

例 次に、出力ポリシー マップとして *plcmap1* を適用する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output plcmap1
```

次に、ポートから *plcmap2* を削除する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no service-policy output plcmap2
```

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	Quality of Service (QoS) ポリシー マップを表示します。
show policy-map interface [interface-id]	(任意) 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に設定されているポリシー マップを表示します。
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 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

service-policy (ポリシーマップクラス コンフィギュレーション)

入力または出力ポリシー マップ、あるいはポート単位、VLAN 単位のポリシー マップに対して Quality of Service (QoS) サービス ポリシーを設定するには、**service-policy** 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。ポリシー マップ内の QoS ポリシーとしてサービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。

service-policy *policy-map-name*

no service-policy *policy-map-name*

構文の説明	<i>policy-map-name</i>	QoS 階層型サービス ポリシーに使用されるサービス ポリシー マップ (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作成されます) の名前。
--------------	------------------------	---

デフォルト サービス ポリシーは定義されていません。

コマンド モード 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	変更箇所
	12.2(53)EX	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 に基づく分類を使用して定義される親入力ポリシーに QoS 子ポリシーを割り当てるために **service-policy input** コマンドを使用できます。これにより、ポート単位、VLAN 単位 QoS の階層型ポリシーを作成できます。

親出力ポリシー マップに、ポリシーマップ クラス コンフィギュレーションで作成されたサービス ポリシーを適用します。これは、階層型ポリシー マッピングを作成します。第 2 レベル (子) ポリシー マップを入力するために **service-policy policy-map-name** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。

入力ポリシー マップでは、**match vlan** クラスマップ コンフィギュレーション コマンドを使用して、VLAN ID に基づく分類でクラスを設定すると、そのクラスに子 QoS ポリシーを関連付ける **service-policy** 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。これは、ポートで着信トラフィックの VLAN ID に基づいて独立した QoS ポリシーを適用する機能を提供します。ポート単位、VLAN 単位の入力 QoS 機能は、2 レベルの階層型入力ポリシーマップを使用する場合に限り、サポートされます。このポリシー マップは、親レベルで VLAN ベースの分類を定義し、子レベルで 1 つまたは複数の該当する VLAN に適用される QoS ポリシーを定義します。入力ポリシー マップでは、ポリシングおよびマーキングなどの、入力ポリシーに使用可能なすべてのアクションを設定できます。

出力ポリシー マップでは、**shape average** もクラス **class-default** に設定されている場合、クラス **class-default** に 1 つの **service-policy** ポリシーマップ クラス コマンドを適用して、階層型ポリシー マップを設定できます。このポリシー マップは、ポートでシェーピングされるトラフィックのサービ

ス ポリシーを指定し、親ポリシー マップとなります。 **queue-limit** ポリシー マップ クラス コマンドを使用したクラスベースのキューイングアクション、およびスケジューリングアクション (**bandwidth**、**shape average**、または **priority** コマンドを使用) で子ポリシーを設定できます。

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

次に、サービス ポリシーを定義し、それを親ポリシー マップに適用して、出力キューの最大帯域幅 (シェーピング) を 90000000 ビット/秒に設定する例を示します。

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

次の例では、子レベルのポリシー マップのクラス マップが音声およびビデオ トラフィックの一致基準を指定して、子ポリシー マップが各トラフィック タイプの入力ポリシーングに対するアクションを設定します。親レベルのポリシー マップは、指定されたポート上の子ポリシー マップが適用される VLAN を指定します。

```
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```



(注)

また、一致基準を **match vlan 100 200 300** と入力した場合でも、同じ結果になります。

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 5000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# set ip precedence 4
Switch(config-pmap-c)# exit

Switch(config)# policy-map parent-customer-1
Switch(config-pmap)# class customer-1-vlan
Switch(config-pmap-c)# service-policy ingress-policy-1
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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
	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	Quality of Service (QoS) ポリシー マップを表示します。

set cos

パケットのレイヤ 2 サービス クラス (CoS) 値を設定するには **set cos** 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。トラフィックのマーキ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。

```
set cos {cos_value | from-field [table table-map-name]}
```

```
no set cos {cos_value | from-field [table table-map-name]}
```

構文の説明

<i>cos_value</i>	トラフィックを分類する IEEE 802.1Q サービス クラス/ユーザのプライオリティ値を入力します。指定できる範囲は 0 ~ 7 です。
<i>from-field</i>	パケットの CoS 値の設定に使用される特定の packets マーキング カテゴリです。パケットマーキング値のマッピングと変換用テーブルマップを使用している場合、このテーブル マップが <i>map-from</i> packets マーキング カテゴリを確立します。 次のオプションがサポートされています。 <ul style="list-style-type: none"> • cos : CoS 値 • dscp : DiffServ コード ポイント (DSCP) 値 • precedence : IP precedence 値
table	(任意) <i>from-field</i> キーワードとともに使用します。指定のテーブルマップに設定された値が CoS 値の設定に使用されることを示します
<i>table-map-name</i>	(任意) table キーワードとともに使用します。CoS 値の指定に使用されるテーブル マップ名です。テーブル マップ名には、最大 64 の英数字を使用できます。

デフォルト

トラフィックのマーキング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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

同じクラスに対して、**set dscp**、**set precedence**、**set qos-group** などの他のすべてのマーキングアクションとともに **set cos** を設定できます。同じクラスにテーブル マップを使用して、拡張パケットのマーキングとともに複数のマーキングアクションを設定する機能のサポートも追加されています。

スイッチに送信されているパケットをマーキングするには、**set cos** コマンドを使用します。スイッチは、CoS 値のマーキングを含むレイヤ 2 ヘッダー情報を利用できます。

match cos クラスマップ コンフィギュレーション コマンドおよび **set cos** ポリシーマップ クラス コンフィギュレーション コマンドを一緒に使用すると、スイッチの相互運用、および CoS マーキングに基づく Quality Of Service (QoS) の提供が可能です。スイッチにより、CoS 値がすでに一致および設定できるため、CoS 値の一致によってレベル 2 とレベル 3 のマッピングを設定できます。

このコマンドを使用して拡張パケット マーキングを行う場合は、*from-field* パケット マーキング オプションを使用して、CoS 値のマッピングと設定を行うことができます。サポートされている *from-field* マーキング カテゴリは、CoS、DSCP、および IP precedence です。

from-field カテゴリを指定したものの **table** キーワードと *table-map-name* を指定していない場合、デフォルトアクションは、*from-field* カテゴリに関連付けられた値を CoS 値としてコピーすることです。たとえば、**set cos precedence** コマンドを入力する場合、precedence 値がコピーされ、CoS 値として使用されます。**set cos dscp** コマンドを入力する場合、DSCP 値がコピーされ、CoS 値として使用されま

例

次に、cos 3 にすべての FTP トラフィックを設定する例を示します。

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
```

次に、クラスへの CoS テーブル マップに DSCP を割り当てる例を示します。

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos dscp table dscp-cos-tablemap
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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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。

set dscp

パケットのタイプ オブ サービス (ToS) バイトに DiffServ コード ポイント (DSCP) 値を設定して IPv4 トラフィックをマーキングするには、**set [ip] dscp** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。トラフィックのマーキ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。

```
set [ip] dscp {dscp_value |from-field [table table-map-name]}
```

```
no set [ip] dscp {dscp_value |from-field [table table-map-name]}
```



(注) **ip dscp** と入力することは、**dscp** と入力することと同じです。

構文の説明

<i>dscp-value</i>	トラフィックを分類するため DSCP 値を入力します。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。
<i>from-field</i>	パケットの DSCP 値の設定に使用される特定の packets マーキング カテゴリです。パケットマーキング値のマッピングと変換用テーブル マップを使用している場合、このテーブル マップが <i>map-from</i> パケットマーキング カテゴリを確立します。 次のオプションがサポートされています。 <ul style="list-style-type: none"> • cos : サービス クラス (CoS) 値 • dscp : DSCP 値。 • precedence : IP precedence 値
table	(任意) <i>from-field</i> キーワードとともに使用します。指定のテーブル マップに設定された値が DSCP 値の設定に使用されることを示します
<i>table-map-name</i>	(任意) table キーワードとともに使用します。DSCP 値の指定に使用されるテーブル マップ名です。テーブル マップ名には、最大 64 の英数字を使用できます。

デフォルト

トラフィックのマーキング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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

同じクラスに対して、**set cos**、**set qos-group** などの他のマーキングアクションとともに **set dscp** を設定できます。同じクラスにテーブル マップを使用して、拡張パケットのマーキングとともに複数のマーキングアクションを設定する機能のサポートも追加されています。

同じパケットをマーク付けする場合に、**set dscp** コマンドを **set precedence** コマンドと組み合わせて使用することはできません。DSCP 値と IP precedence 値は、相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

DSCP ビットを設定すると、他の Quality of Service (QoS) 機能がビット設定で動作するようになります。

マーキングされたトラフィックには、ネットワークによってプライオリティ（または緊急処理のタイプ）が設定されます。一般に、ネットワークのエッジ（または管理ドメイン）で DSCP 値を設定します。これにより、データが優先順位に従ってキューに格納されます。クラスベース均等化キューイング (CBWFQ) は、輻輳ポイントで優先順位の高いトラフィックの処理を高速化できます。Weighted Tail Drop (WTD) により、輻輳時の優先順位の高いトラフィックの損失率を他のトラフィックより確実に小さくできます。

数値の代わりに、予約済みキーワード **EF**、**AF11**、および **AF12** を使用して、*dscp* 値を指定することもできます。

このコマンドを使用して拡張パケット マーキングを行う場合は、*from-field* パケット マーキング オプションを使用して、DSCP 値のマッピングと設定を行うことができます。サポートされている *from-field* マーキング カテゴリは、CoS、DSCP、および IP precedence です。

from-field カテゴリを指定したものの **table** キーワードと *table-map-name* を指定していない場合、デフォルトアクションは、*from-field* カテゴリに関連付けられた値を DSCP 値としてコピーすることです。たとえば、**set dscp cos** コマンドを入力する場合、CoS 値がコピーされ、DSCP 値として使用されます。

例

次に、DSCP 10 にすべての FTP トラフィックを設定する例を示します。

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

次に、クラスへの DSCP テーブル マップに CoS を割り当てる例を示します。

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp cos table cos-dscp-tablemap
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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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。

set precedence

パケットの IP precedence 値を設定して IPv4 トラフィックをマーキングするには、**set [ip] precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。トラフィックのマーキ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。

```
set [ip] precedence {precedence_value | from-field [table table-map-name]}
```

```
no set [ip] precedence {precedence_value | from-field [table table-map-name]}
```



(注)

ip precedence と入力することは、**precedence** と入力することと同じです。

構文の説明

<i>precedence_value</i>	トラフィックを分類するため IPv4 precedence 値を入力します。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ク名を入力することもできます。
<i>from-field</i>	パケットの precedence 値の設定に使用される特定の packets マーキング カテゴリです。パケットマーキング値のマッピングと変換用テーブル マップを使用している場合、このテーブル マップが <i>map-from</i> パケットマーキング カテゴリを確立します。 次のオプションがサポートされています。 <ul style="list-style-type: none"> • cos : サービス クラス (CoS) 値 • dsep : DiffServ コード ポイント (DSCP) 値 • precedence : IP precedence 値
table	(任意) <i>from-field</i> キーワードとともに使用します。指定のテーブル マップに設定された値が precedence 値の設定に使用されることを示します
<i>table-map-name</i>	(任意) table キーワードとともに使用します。precedence 値の指定に使用されるテーブル マップ名です。テーブル マップ名には、最大 64 の英数字を使用できます。

デフォルト

トラフィックのマーキング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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

同じクラスに対して、**set cos**、**set qos-group** などの他のマーキングアクションとともに **set precedence** を設定できます。同じクラスにテーブル マップを使用して、拡張パケットのマーキングとともに複数のマーキングアクションを設定する機能のサポートも追加されています。

同じパケットをマーク付けする場合に、**set precedence** コマンドを **set dscp** コマンドと組み合わせて使用することはできません。DSCP 値と IP precedence 値は、相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

precedence ビットを設定すると、他の Quality of Service (QoS) 機能がビット設定で動作するようになります。

マーキングされたトラフィックには、ネットワークによってプライオリティ（または緊急処理のタイプ）が設定されます。一般に、ネットワークのエッジ（または管理ドメイン）で **precedence** 値を設定します。これにより、データが優先順位に従ってキューに格納されます。クラスベース均等化キューイング (CBWFQ) は、輻輳ポイントで優先順位の高いトラフィックの処理を高速化できます。

Weighted Tail Drop (WTD) により、輻輳時の優先順位の高いトラフィックの損失率を他のトラフィックより確実に小さくできます。

数値の代わりに、予約済みキーワード **EF**、**AF11**、および **AF12** を使用して、*dscp* 値を指定することもできます。

このコマンドを使用して拡張パケット マーキングを行う場合は、*from-field* パケット マーキング オプションを使用して、**precedence** 値のマッピングと設定を行うことができます。サポートされている *from-field* マーキング カテゴリは、CoS、DSCP、および IP precedence です。

from-field カテゴリを指定したものの **table** キーワードと *table-map-name* を指定していない場合、デフォルトアクションは、*from-field* カテゴリに関連付けられた値を **precedence** 値としてコピーすることです。たとえば、**set precedence cos** コマンドを入力する場合、CoS 値がコピーされ、**precedence** 値として使用されます。

例

次に、すべての FTP トラフィックに IP precedence 値 5 を指定する例を示します。

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set precedence 5
Switch(config-pmap-c)# exit
```

次に、クラスへの **precedence** テーブル マップに CoS を割り当てる例を示します。

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set precedence cos table cos-prec-tablemap
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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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。

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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。

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	変更箇所
12.2(53)EX	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

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
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/2	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*

The following configuration command script was created:

```
hostname host-name
enable secret 5 $1$LlBw$0XclwyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
!
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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
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。

shape average

shape average 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、平均トラフィックシェーピング レートを指定することによって、クラスベースまたはポートのシェーピングを設定します。ポートシェーピングを設定するには、クラス **class-default** とともにコマンドを使用します。トラフィックシェー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。

shape average target bps

no shape average target bps

構文の説明	<i>target bps</i>	ビット/秒 (bps) 単位でのターゲット平均ビット レート。指定できる範囲は、クラスベースシェーピングでは 64000 ~ 1000000000、ポートシェーピングでは 4000000 ~ 1000000000 です。
--------------	-------------------	--

デフォルト トラフィックシェーピング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	変更箇所
	12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン 出力トラフィックを制御するには、**shape average** ポリシーマップ クラス コマンドを使用します。シェーピングは、入力ポリシーマップでサポートされません。

トラフィックシェーピングは、データの転送レートを制限します。クラスベースシェーピングでユーザ定義クラスまたは **class-default** のトラフィックシェーピングを設定すると、そのクラスの最大情報レート (PIR) が設定されます。インターフェイスに適用されているポリシーマップ内の唯一のクラスであるクラス **class-default** に対してトラフィックシェーピングを設定すると、そのインターフェイスの PIR が設定されます (ポートシェーピング)。

プライオリティキューイングを含むクラスでは、**shape average** を設定できません (**priority** ポリシーマップ クラス コンフィギュレーション コマンドで設定されます)。

shape average コマンドはクラスのデフォルトのキュー制限を使用します。**queue-limit** ポリシーマップ クラス コマンドを使用してキュー制限を変更することによって、**shape average** コマンドで設定されたデフォルトを上書きできます。

bandwidth 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クラスベース均等化キューイング (CBWFQ) を設定し、その同じクラスに対して **shape average** コマンドを使用してトラフィックシェーピングを設定することはできません。

クラス **class-default** に **shape average** も設定されている場合にのみ、クラス **class-default** に **service-policy** ポリシーマップ クラス コマンドを適用して階層型ポリシーマップを設定できます。

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

次に、ファストイーサネットポート上で発信トラフィックのトラフィックシェーピングを設定し、*outclass1*、*outclass2*、および *outclass3* がバッファサイズのうち最大 50 Mb/s、20 Mb/s、10 Mb/s を取得する例を示します。クラスの **class-default** は、残りのポート帯域幅を取得します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy out out-policy
```

次に、前述の例で設定された *out-policy* ポリシーマップに基づいて割り当てられ、ポートを 90 Mb/s にシェーピングする階層型ポリシーマップを設定して、ポートシェーピングを設定する例を示します。

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
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。

関連コマンド

コマンド	説明
class	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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。
show policy-map interface [<i>interface-id</i>]	(任意) 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に設定されているポリシーマップを表示します。

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

<i>name</i>	(任意) ACL の名前です。
<i>number</i>	(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) Interprocess Communication (IPC; プロセス間通信) 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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tring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	変更箇所
12.2(53)EX	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 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。

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
```

show access-lists

```
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
```

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。構文情報については、『 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 』> 「 IP Services Commands 」を選択してください。
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。構文情報については、『 Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 』> 「 IP Services Commands 」を選択してください。
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 alarm description port

テキストの説明とアラーム番号を表示するには、**show alarm description port** ユーザ EXEC コマンドを使用します。

```
show alarm description port [ | {begin | exclude | include} expression]
```

構文の説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 alarm description port** コマンドの出力を示します。出力では、アラーム ID とそれぞれに対応するアラームの説明を示します。

```
Switch> show alarm description port
 1      Link Fault
 2      Port Not Forwarding
 3      Port Not Operating
 4      FCS Error Rate exceeds threshold
```

関連コマンド

コマンド	説明
alarm profile (グローバル コンフィギュレーション)	アラーム ID およびアラーム オプションが 1 つ以上含まれるアラーム プロファイルを作成します。
show alarm profile	アラーム プロファイルすべてまたは指定したアラーム プロファイルを表示し、それぞれのプロファイルが関連付けられているインターフェイスをリスト表示します。

show alarm profile

システムに設定されたアラーム プロファイルすべて、または指定されたプロファイルとプロファイルが関連付けられたインターフェイスを表示するには、**show alarm profile** ユーザ EXEC コマンドを使用します。

show alarm profile [*name*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

<i>name</i>	(任意) 指定された名前のプロファイルのみを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

プロファイル名を入力しない場合、既存のアラーム プロファイルすべてのプロファイル情報が表示されます。このコマンドでは、デフォルト設定は表示されません。

デフォルトでは、*defaultPort* プロファイルはすべてのインターフェイスに適用されています。このプロファイルによって、ポートが動作していない (3) アラームのみがイネーブルになります。このプロファイルを変更して他のアラームをイネーブルにするには、**alarm profile defaultPort** 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。

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 alarm profile** コマンドの出力を示します。

この出力では設定されたプロファイルに関連付けられたポートすべてが表示されます。

```
Switch> show alarm profile GigE-UplinkPorts
Interface      Gil/2
Alarms         1,2,3,4
Syslog         1,2,3,4
Notifies       1,2,3,4
Relay-major    4
Relay-minor    1,2
```

この出力では設定されたプロファイルすべてが表示されます。

```
Switch> show alarm profile
Alarm Profile my_gig_port:
Interface      Gil/2
Alarms         1,2,3,4
Syslog         1,2,3,4
```

■ show alarm profile

```

Notifies          1,2,3,4
Relay-major       4
Relay-minor       1,2
Alarm Profile my_fast_port:
Interface         Fa1/1
Alarms            1,2,3,4
Syslog            1,2,3,4
Notifies          1,2,3,4
Relay-major       4
Relay-minor       1,2

```

■ 関連コマンド

コマンド	説明
alarm profile (グローバル コンフィギュレーション)	アラーム ID およびアラーム オプションが 1 つ以上含まれるアラーム プロファイルを作成します。
alarm profile (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アラーム プロファイルを関連付けます。

show alarm settings

スイッチの環境アラーム設定すべてを表示するには、**show alarm settings** ユーザ EXEC コマンドを使用します。

show alarm settings [| {**begin** | **exclude** | **include**} *expression*]

構文の説明	
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
	12.2(53)EX	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 alarm settings** コマンドの出力を示します。出力では、スイッチ上のスイッチアラーム設定すべてが表示されます。

```
Switch> show alarm settings
Power Supply
  Alarm           Disabled
  Relay           Disabled
  Notifies        Disabled
  Syslog          Disabled
Temperature-Primary
  Alarm           Enabled
  Thresholds      MAX: 95C          MIN: -20C
  Relay           MAJ
  Notifies        Enabled
  Syslog          Enabled
Temperature-Secondary
  Alarm           Disabled
  Threshold
  Relay
  Notifies        Disabled
  Syslog          Disabled
```

関連コマンド	コマンド	説明
	alarm facility power-supply	電源アラーム オプションを設定します。
	alarm facility temperature	温度アラーム オプションを設定します。

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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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、**show archive status** 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。

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。

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	
<i>acl-name</i>	(任意) ACL の名前です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
	12.2(53)EX	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 <i>interface-id</i>	(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 <i>method</i>	(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 <i>session-id</i>	(任意) 認証マネージャのセッションを指定します。
handle <i>handle</i>	(任意) 1 ~ 4294967295 の範囲を指定します。
mac <i>mac</i>	(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	変更箇所
12.2(53)EX	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 2-6 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。終了ステータスのセッションでは、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 2-6 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 2-6 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 2-7 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 2-7 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想されています。
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 gigabitethernet1/23
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 0908140400000007003651EC
Gi3/46 (unknown) N/A DATA Authz Success 09081404000000080057C274
```

show authentication

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 gi 3/46
      Interface: GigabitEthernet3/46
      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: 0908140400000080057C274
      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: GigabitEthernet1/23
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 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タスの手動制御をイネーブルにします。
authentication port-control	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 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。

```
Switch# show boot
5d05h: %SYS-5-CONFIG_I: Configured from console by console
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break       : no
Manual Boot        : yes
HELPER path-list   :
Auto upgrade       : yes
```

表 2-8 に、表示される各フィールドの説明を示します。

表 2-8 show boot のフィールドの説明

フィールド	説明
BOOT path-list	<p>自動ブート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。</p> <p>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。</p> <p>BOOT 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かった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとしています。</p>
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	ブート中のブレイクがイネーブルか、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ブレイク キーを押すと、自動ブート プロセスを中断できます。
Manual Boot	スイッチが自動でブートするか、または手動でブート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 ロダはシステムを自動的に起動しようとしています。他の値に設定されている場合は、ブート ロダ 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。

関連コマンド	コマンド	説明
	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	次回のブート サイクル時のスイッチの手動ブート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	次回の起動時に読み込む 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]
```



(注)

TDR は、Cisco CGS 2520 スイッチ上の銅線イーサネット 10/100 ポートでのみサポートされています。

構文の説明

<i>interface-id</i>	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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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、Cisco CGS 2520 スイッチ上の銅線イーサネット 10/100 ポートでのみサポートされています。小型フォーム ファクタ (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、Cisco CGS 2520 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 fastethernet0/1
TDR test last run on: March 01 18:14:44
```

```
Interface Speed Local pair Pair length Remote pair Pair status
-----
Fa0/1      100M   Pair A    4    +/- 5 meters Pair A    Normal
          Pair B    4    +/- 5 meters Pair B    Normal
          Pair C    N/A                      Pair C    N/A
          Pair D    N/A                      Pair D    N/A
```

表 2-9 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 2-9 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。 <ul style="list-style-type: none"> 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 100 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 <ul style="list-style-type: none"> 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 が動作しているときの **show interfaces interface-id** コマンドの出力を示します。

```
Switch# show interface fastethernet0/1
fastethernet0/1 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 fastethernet0/1
% TDR test was never issued on fa0/1
```

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 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

<i>class-map-name</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 access-group	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 controllers cpu-interface

CPU ネットワーク インターフェイス ASIC のステータスを表示し、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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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
```

show controllers cpu-interface

```

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 19CDD00 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**}] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

<i>interface-id</i>	物理インターフェイス (タイプ、モジュール、ポート番号など)
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) 機能の動作ステータスを表示に含めます。
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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

すべてのインターフェイス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ブルシューティング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。

show controllers ethernet-controller

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 2-10 に *Transmit* フィールドの説明を示し、表 2-11 に *Receive* フィールドの説明を示します。

```
Switch# show controllers ethernet-controller gigabitethernet0/1
Transmit GigabitEthernet0/1          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 2-10 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 2-10 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 2-11 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 2-11 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上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。出力の最後の行がインターフェイスの Auto-MDIX 設定であることを注意してください。

```

Switch# show controllers ethernet-controller gigabitethernet0/2 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 Register : 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、**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
=====
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

```

show controllers ethernet-controller

```

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
=====
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
=====
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 Content Addressable Memory (TCAM) と CAM コントローラである TCAM インターフェイス ASIC のレジスタステータスを表示します。

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] [ | {begin | exclude | include} expression]
```

構文の説明

<i>instance</i>	(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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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、スイッチに対する **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
Current State          : 55 55 51 51 00 00
Current Event          : 11 11 10 10 00 00
Timers                 : 00 00 00 00 00 0E 00 11 00 00 00 00
Error State            : 00 00 00 00 00 00
Error Code             : 00 00 00 00 00 00 00 00 00 00 00
Power Status           : Y Y Y Y N Y N N N N N
Auto Config            : Y Y Y Y Y Y Y N N N N
Disconnect             : N N N N N N N N N N N
Detection Status       : 03 33 30 30 00 00
Current Class          : 03 33 30 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 spanning-tree	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 Content Addressable Memory (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 のレジスタの状態を表示するには、**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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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

<i>interface-id</i>	(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 <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) 指定された <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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
Fa0/1         0                    0
Fa0/2         0                    0
Fa0/3         0                    0
Fa0/4         0                    0
Fa0/5         0                    0
Fa0/6         0                    0
Fa0/7         0                    0
```

<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 gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization : 0
Transmit Bandwidth Percentage Utilization : 0
```

表 2-12 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 cpu traffic qos

CPU 生成トラフィックの QoS マーキング値を表示するには、ユーザ EXEC モードで **show cpu traffic qos** コマンドを使用します。

```
show cpu traffic qos [ [ begin | exclude | include expression ]
```

構文の説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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

すべての CPU 生成トラフィックの QoS マーキング値を表示します。

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	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

次に、**show cpu traffic qos** コマンドの出力例を示します。

```
Switch> show cpu traffic qos
QOS - CPU Generated Traffic
-----
Set parameter-type      To parameter-value/From
      parameter-type based on table-map
-----
Cos                      cos
      precedence table-map map1
DSCP                     Default
Precedence               dscp
Qos Group                5
```

関連コマンド

コマンド	説明
class-map	指定した基準とパケットのマッチングに使用されるクラス マップを設定し、クラスマップ コンフィギュレーション モードを開始します。
cpu traffic qos cos	コントロールプレーン トラフィックのサービス クラス (CoS) マーキングを設定します。
cpu traffic qos dscp	コントロールプレーン トラフィックの DSCP に基づく Quality of Service (QoS) マーキングを設定します。
cpu traffic qos precedence	コントロールプレーン トラフィックの優先順位に基づく Quality of Service (QoS) マーキングを設定します。
cpu traffic qos qos-group	サービス クラス (CoS)、IP DiffServ コード ポイント (DSCP)、または IP-precedence パケット マーキングを変更せずに、すべての CPU 生成 トラフィックを出力ポリシーマップの 1 つのクラスにマッピングします。
policy-map	複数の物理ポートに適用できるポリシー マップを設定し、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 policy-map	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシーマップ クラスの QoS ポリシー マップ情報を表示 します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。
show table-map	すべての設定済みテーブル マップまたは指定されたテーブル マップの情 報を表示します。
table-map	Quality of Service (QoS) マッピングを設定し、テーブルマップ コン フィギュレーション モードを開始します。

show diagnostic

オンライン診断テストの結果およびサポートされるテスト スイッチを表示するには、**show diagnostic** ユーザ EXEC コマンドを使用します。

show diagnostic content [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic post [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic result [test {*name* | *test-id* | *test-id-range* | **all**}] [detail] [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic schedule [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic status [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic switch [detail] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

content	特定のテストおよびスイッチに関して、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。
post	Power-on Self-Test (POST; 電源投入時自己診断テスト) の結果を表示します。
result	診断テストの結果を表示します。
test	(任意) 表示するテスト結果を指定します。 <ul style="list-style-type: none"> • <i>name</i> : 診断テストの名前を入力して、そのテストの結果だけを表示します。 • <i>test-id</i> : テスト ID 番号を入力して、そのテストの結果だけを表示します。テスト ID は 1 ~ 6 です。 • <i>test-id-range</i> : テスト ID 番号の範囲を入力して、該当するテストの結果だけを表示します。 • all : このキーワードを入力して、すべてのテストの結果を表示します。
detail	(任意) 詳細なテスト結果を表示します。
schedule	スケジューリングされている診断テストを表示します。
status	実行中の診断テストを表示します。
switch	スイッチの診断結果を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 diagnostic post コマンドの出力は、**show post** コマンドの出力と同じです。

show diagnostic result [detail] コマンドの出力は **show diagnostic switch [detail]** コマンドの出力と同じです。

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、診断テストの ID および属性を表示する方法を示します。

```
Switch> show diagnostic content
:
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
```

ID	Test Name	Attributes	Test Interval day hh:mm:ss.ms	Thres hold
1)	TestPortAsicStackPortLoopback	B*N***I**	not configured	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、スイッチの診断テスト結果を表示する方法を示します。これらの結果を表示するには、**show diagnostic switch** コマンドも使用できます。

```
Switch> show diagnostic result
SerialNo : CGS2520ABCD1234

Overall diagnostic result: PASS

Test results: (.= Pass, F = Fail, U = Untested)

1) TestPortAsicStackPortLoopback ---> .
2) TestPortAsicLoopback -----> U
3) TestPortAsicCam -----> U
4) TestPortAsicRingLoopback -----> U
5) TestMicRingLoopback -----> U
6) TestPortAsicMem -----> U
```

show diagnostic

次の例では、スタックで実行中のテスト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                             N/A
2      TestPortAsicStackPortLoopback             <OD>
      TestPortAsicLoopback                     <OD>
      TestPortAsicCam                           <OD>
      TestPortAsicRingLoopback                 <OD>
      TestMicRingLoopback                       <OD>
      TestPortAsicMem                           <OD>
3      N/A                                         N/A                             N/A
4      N/A                                         N/A                             N/A
=====
```

<output truncated>

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
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.
```

次に、スイッチの詳細な結果を表示する方法を示します。これらの結果を表示するには、**show diagnostic result all detail** コマンドも使用できます。

```
Switch> show diagnostic switch detail
Switch:   SerialNo : CGS2520ABCD1234
```

Overall diagnostic result: PASS

Test results: (.= Pass, F = Fail, U = Untested)

1) TestPortAsicStackPortLoopback ---> .

```
Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 19
Last test execution time ----> Mar 01 1993 00:21:46
First test failure time ----> n/a
Last test failure time ----> n/a
Last test pass time -----> Mar 01 1993 00:21:46
Total failure count -----> 0
Consecutive failure count ---> 0
```

2) TestPortAsicLoopback -----> U

```
Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 0
Last test execution time ----> n/a
First test failure time ----> n/a
Last test failure time ----> n/a
Last test pass time -----> n/a
Total failure count -----> 0
Consecutive failure count ---> 0
```

```

3) TestPortAsicCam -----> U

   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 0
   Last test execution time ----> n/a
   First test failure time ----> n/a
   Last test failure time ----> n/a
   Last test pass time -----> n/a
   Total failure count -----> 0
   Consecutive failure count ---> 0

```

```

4) TestPortAsicRingLoopback -----> U

   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 0
   Last test execution time ----> n/a
   First test failure time ----> n/a
   Last test failure time ----> n/a
   Last test pass time -----> n/a
   Total failure count -----> 0
   Consecutive failure count ---> 0

```

```

5) TestMicRingLoopback -----> U

   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 0
   Last test execution time ----> n/a
   First test failure time ----> n/a
   Last test failure time ----> n/a
   Last test pass time -----> n/a
   Total failure count -----> 0
   Consecutive failure count ---> 0

```

```

6) TestPortAsicMem -----> U

   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 0
   Last test execution time ----> n/a
   First test failure time ----> n/a
   Last test failure time ----> n/a
   Last test pass time -----> n/a
   Total failure count -----> 0
   Consecutive failure count ---> 0

```

関連コマンド

コマンド	説明
diagnostic monitor	ヘルス モニタリング診断テストを設定します。
diagnostic schedule test	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 test	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]

このコマンドは、スイッチでメトロ IP アクセス イメージまたはメトロ アクセス イメージが稼動している場合にのみ表示されます。

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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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)
-----
Gi0/1
Gi0/2
Gi0/3
Gi0/6
Po2

Switch> show dot1q-tunnel interface gigabitethernet0/1
dot1q-tunnel mode LAN Port(s)
-----
Gi0/1
```

関連コマンド

コマンド	説明
show vlan dot1q tag native	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** 特権 EXEC コマンドを使用します。

```
show dot1x [all | interface interface-id | statistics interface interface-id] [| {begin |
exclude | include} expression]
```

構文の説明

all	(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	(任意) 指定のポート (タイプ、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。
statistics interface interface-id	(任意) 指定のポート (タイプ、モジュール、ポート番号を含む) の IEEE 802.1x の統計情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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。

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** および **show dot1x all** 特権 EXEC コマンドの出力を示します。

```
Switch# show dot1x
Sysauthcontrol                = Enabled
Dot1x Protocol Version       = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

```
Switch# show dot1x all
Dot1x Info for interface GigabitEthernet0/1
```

```
-----
Supplicant MAC 00d0.b71b.35de
  AuthSM State      = CONNECTING
  BendSM State      = IDLE
PortStatus          = UNAUTHORIZED
MaxReq              = 2
HostMode            = Single
Port Control        = Auto
```

show dot1x

```

QuietPeriod      = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod     = 3600 Seconds
ServerTimeout    = 30 Seconds
SuppTimeout      = 30 Seconds
TxPeriod         = 30 Seconds
Guest-Vlan       = 0

```

Dot1x Info for interface GigabitEthernet0/2

```

-----
PortStatus       = UNAUTHORIZED
MaxReq           = 2
HostMode         = Multi
Port Control     = Auto
QuietPeriod      = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod     = 3600 Seconds
ServerTimeout    = 30 Seconds
SuppTimeout      = 30 Seconds
TxPeriod         = 30 Seconds
Guest-Vlan       = 0

```

次の例では、**show dot1x interface interface-id** 特権 EXEC コマンドの出力を示します。

```

Switch# show dot1x interface gigabitethernet0/1
Supplicant MAC 00d0.b71b.35de
  AuthSM State      = AUTHENTICATED
  BendSM State      = IDLE
PortStatus         = AUTHORIZED
MaxReq             = 2
HostMode           = Single
Port Control       = Auto
QuietPeriod        = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod       = 3600 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
TxPeriod           = 30 Seconds
Guest-Vlan         = 0

```

次の例では、**show dot1x statistics interface interface-id** コマンドの出力を示します。表 2-13 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 statistics interface gigabitethernet0/1
PortStatistics Parameters for Dot1x
-----
TxReqId = 15   TxReq = 0       TxTotal = 15
RxStart = 4    RxLogoff = 0    RxRespId = 1   RxResp = 1
RxInvalid = 0  RxLenErr = 0    RxTotal = 6
RxVersion = 1  LastRxSrcMac 00d0.b71b.35de

```

表 2-13 show dot1x statistics のフィールドの説明

フィールド	説明
TxReqId	送信された Extensible Authentication Protocol (EAP) -Request/Identity 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
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
RxStart	受信された有効な Extensible Authentication Protocol over LAN (EAPOL) -Start フレームの数

表 2-13 show dot1x statistics のフィールドの説明 (続き)

フィールド	説明
RxLogoff	受信された EAPOL-Logoff フレームの数
RxRespId	受信された EAP-Response/Identity 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
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
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	設定可能な IEEE 802.1x パラメータをデフォルト値に戻します。

show env

スイッチのアラーム接点、温度、および電源情報を表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show env** コマンドを使用します。

```
show env {alarm-contact | all | power | temperature} [| {begin | exclude | include}
expression]
```

構文の説明

alarm-contact	アラーム接点のステータスを表示します。
all	温度、電源およびアラーム ステータスを表示します。
power	スイッチの電源のステータスを表示します。
temperature	スイッチの温度のステータスを OK または FAULTY として表示します。また、温度のしきい値を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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 およびユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	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 env alarm-contact** コマンドの出力を示します。

```
Switch# show env alarm-contact
ALARM CONTACT 1
  Status:      asserted
  Description: main_lab_door
  Severity:    critical
  Trigger:     open
ALARM CONTACT 2
  Status:      asserted
  Description: main_lab_cabinet-1_door
  Severity:    major
  Trigger:     open
ALARM CONTACT 3
  Status:      asserted
  Description: main_lab_supply-room_door
  Severity:    major
  Trigger:     open
ALARM CONTACT 4
  Status:      not asserted
  Description: main_lab_water-level_FLOOD
```

```
Severity:    critical
Trigger:    closed
```

次の例では、**show env all** コマンドの出力を示します。

```
Switch# show env all
TEMPERATURE is OK
Temperature Value: 39 Degree Celsius
POWER SUPPLY 1A TEMPERATURE is Failure-Thermal POWER SUPPLY 1B TEMPERATURE is OK POWER
SUPPLY 1A Temperature Value: 97 Degree Celsius POWER SUPPLY 1A Critical Temperature
Thresh: 110 Degree Celsius POWER SUPPLY 1A Over Temperature Thresh: 95 Degree Celsius
POWER SUPPLY 1B Temperature Value: 45 Degree Celsius POWER SUPPLY 1B Critical Temperature
Thresh: 110 Degree Celsius POWER SUPPLY 1B Over Temperature Thresh: 95 Degree Celsius

SW  PID                      Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -----                      -
1A  PWR-150-HV                  DTM1348000B Failure-Thermal Good      Good     75/65
1B  PWR-150-HV                  DTM1348000C OK              Good      Good     75/65

ALARM CONTACT 1 is not asserted
ALARM CONTACT 2 is not asserted
ALARM CONTACT 3 is not asserted
ALARM CONTACT 4 is not asserted
```

これは、電源 1A に接続された AC 入力がない場合の **show env power** コマンドの出力例を示します。

```
Switch# show env power
TEMPERATURE is OK
POWER SUPPLY 1A TEMPERATURE is Disabled
POWER SUPPLY 1B TEMPERATURE is OK
```

これは、2 台の AC 電源が存在する場合の **show env power** コマンドの出力例を示します。

```
Switch# show env power
SW  PID                      Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -----                      -
1A  PWR-150-HV                  DTM1348000B Failure-Thermal Good      Good     75/65
1B  PWR-150-HV                  DTM1348000C OK              Good      Good     75/65
```

次の例では、**show env temperature** コマンドの出力を示します。

```
Switch# show env temperature
TEMPERATURE is OK
POWER SUPPLY 1A TEMPERATURE is Failure-Thermal
POWER SUPPLY 1B TEMPERATURE is OK
```

関連コマンド

コマンド	説明
alarm contact	アラーム接点を設定します。

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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

Mode 列は、errdisable 理由で設定されたシャットダウン モードを示します。

- **port** : 違反が発生した場合、物理ポートが **errdisable** になります。
- **vlan** : 違反が発生した場合、仮想ポートがディセーブルになります。
- **port/vlan** : 一部のポートは物理ポートのディセーブルに設定され、他のポートは仮想ポートのディセーブルに設定されています。各ポートの設定を表示するには、**show running config** 特権 EXEC コマンドを入力します。

表示された Reason 列の gbic-invalid エラーの理由は、無効な小型フォーム ファクタ (SFP) 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 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    port
channel-misconfig   Enabled    port
community-limit     Enabled    port
dhcp-rate-limit     Enabled    port
dtp-flap            Enabled    port
gbic-invalid        Enabled    port
invalid-policy      Enabled    port
l2ptguard           Enabled    port
link-flap           Enabled    port
link-monitor-fail   Enabled    port
loopback            Enabled    port
lsgroup             Enabled    port
```

```

oam-remote-failure    Enabled    port
pagp-flap             Enabled    port
psecure-violation     Enabled    port/vlan
security-violatio     Enabled    port
sfp-config-mismatch   Enabled    port
storm-control         Enabled    port
udld                  Enabled    port
vmps                  Enabled    port

```



(注)

ntp-flap、ilpower、storm-control、および unicast-flood の各フィールドは、出力には表示されますが、無効です。

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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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くと、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; ダイナミック トランッキング プロトコル) ステート (ポート モード アクセス/トランク)、または Port Aggregation Protocol (PAgP; ポート集約プロトコル) 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



(注)

出力表示に表示されますが、スイッチは DTP をサポートしません。

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 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。

gbic-invalid error-disable の理由は、無効な小型フォーム ファクタ (SFP) モジュール インターフェイスを意味します。

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
l2ptguard              Disabled
link-flap              Enabled
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)
-----
Gi0/2         link-flap          279
```



(注) unicast-flood フィールドおよび DTP 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

チャンネルの 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

<i>channel-group-number</i>	(任意) チャンネル 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 チャン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	ポートチャン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	各チャンネル グループのサマリーを 1 行で表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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-group を指定しない場合は、すべてのチャンネル グループが表示されます。

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 チャン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ンネル グループ内で設定されていること（および間接的にチャンネル グループ内で唯一のポート チャンネルであること）を意味します。



(注)

スイッチでは、レイヤ 3 ポートをサポートするため、メトロ IP アクセス イメージが稼動している必要があります。

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 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: Gi0/1
-----

Port state      = Up Mstr In-Bndl
Channel group   = 1           Mode = Active           Gchange = -
Port-channel    = Po1         GC = -             Pseudo port-channel = Po1
Port index      = 0           Load = 0x00         Protocol = LACP

Flags:  S - Device is sending Slow LACPDU      F - Device is sending fast LACPDU
        A - Device is in active mode.           P - Device is in passive mode.

Local information:

Port      Flags   State      LACP port   Admin   Oper   Port   Port
Gi0/1    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    Gi0/1     Active        0
0      00    Gi0/2     Active        0

Time since last port bundled: 01d:20h:20m:20s   Gi0/2
```

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
```

show etherchannel

```

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Pol(SU)         LACP     Gi0/1(P)  Gi0/2(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: Pol      (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    Gi0/1     Active        0
0      00    Gi0/2     Active        0

Time since last port bundled:  01d:20h:24m:44s  Gi0/2

```

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 ethernet loopback

スイッチまたはインターフェイスで設定されているポート単位のイーサネット ループバックの情報を表示するには、**show ethernet loopback** 特権 EXEC コマンドを使用します。

```
show ethernet loopback [interface-id] [| {begin | exclude | include} expression]
```

構文の説明

<i>interface-id</i>	(任意) 指定したインターフェイスのループバック情報を表示します。イーサネット ループバックは物理インターフェイスだけでサポートされます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 を指定しない場合は、すべての設定済みループバックが表示されます。スイッチは最大 2 つのイーサネット ループバック設定をサポートします。

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 ethernet loopback** コマンドの出力を示します。

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Gi0/3
Status              : configured
MAC Mode            : swap
Time out            : 60
```

show ethernet loopback

次の例では、ポートおよび VLAN の両方のループバック セッションが設定および開始されている場合の出力を示します。

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Fa0/1
Direction          : facility
Type               : port
Status             : active
MAC Mode           : swap
Time out           : none
=====
Loopback Session 1 : Interface Fa0/2
Direction          : facility
Type               : vlan
Status             : active
MAC Mode           : copy
Vlan               : 3
Time out           : 100
```

関連コマンド

コマンド	説明
ethernet loopback (イーサネット コンフィギュレーション)	インターフェイス上のイーサネット ループバック操作を設定します。
ethernet loopback (特権 EXEC)	ループバック操作を開始または中止します。

show ethernet service evc

Ethernet Virtual Connection (EVC; イーサネット仮想接続) カスタマーサービス インスタンスについての情報を表示するには、**show ethernet service evc** 特権 EXEC コマンドを使用します。

```
show ethernet service evc [id evc-id | interface interface-id] [detail] [| {begin | exclude | include} expression]
```

構文の説明

id <i>evc-id</i>	(任意) 指定したサービスの EVC 情報を表示します。EVC ID に設定できる文字列は 1 ~ 100 文字です。
interface <i>interface-id</i>	(任意) 指定したインターフェイスの EVC 情報を表示します。
detail	(任意) EVC サービスか、指定された EVC ID またはインターフェイスについての詳細情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 ethernet service evc** コマンドの出力を示します。

```
Switch# show ethernet service evc
Identifier          Type  Act-UNI-cnt  Status
BLUE                P-P   2            Active
PINK                MP-MP  2            PartiallyActive
PURPLE              P-P   2            Active
BROWN               MP-MP  2            Active
GREEN               P-P   3            Active
YELLOW              MP-MP  2            PartiallyActive
BANANAS             P-P   0            InActive
TEST2               P-P   0            NotDefined
ORANGE              P-P   2            Active
TEAL                P-P   0            InActive
```

関連コマンド

コマンド	説明
ethernet evc <i>evc-id</i>	EVC を定義し、EVC コンフィギュレーション モードを開始します。

show ethernet service instance

イーサネット カスタマーサービス インスタンスについての情報を表示するには、**show ethernet service instance** 特権 EXEC コマンドを使用します。

show ethernet service instance [*id id*] [*interface interface-id*] [*detail*] [| {*begin* | *exclude* | *include*} *expression*]

構文の説明

id <i>id</i>	(任意) VLAN にマップが適用されないインターフェイス単位のサービス ID である、指定されたサービス インスタンス ID を定義します。指定できる範囲は 1 ~ 4294967295 です。
interface <i>interface-id</i>	(任意) 指定したインターフェイスのサービスインスタンス情報を表示します。
detail	(任意) サービス インスタンスか、指定されたサービス インスタンス ID またはインターフェイスについての詳細情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 ethernet service instance** コマンドの出力を示します。

```
Switch# show ethernet service instance
Identifier Interface          CE-Vlans
222      FastEthernet0/1          untagged,1-4094
10       FastEthernet0/2
222      FastEthernet0/2          200
333      FastEthernet0/2          default
10       FastEthernet0/3          300
11       FastEthernet0/3
10       FastEthernet0/4          300
10       FastEthernet0/6          untagged,1-4094
10       FastEthernet0/7          untagged,1-4094
10       FastEthernet0/8          untagged,1-4094
10       FastEthernet0/9          untagged
20       FastEthernet0/9
222      FastEthernet0/11         300-350,900-999
333      FastEthernet0/11         100-200,1000,1999-4094
222      FastEthernet0/12         20
```

333	FastEthernet0/12	10
10	FastEthernet0/13	10
20	FastEthernet0/13	20
30	FastEthernet0/13	30
200	FastEthernet0/13	222
200	FastEthernet0/14	200,222
300	FastEthernet0/14	333
555	FastEthernet0/14	555

関連コマンド

コマンド	説明
<code>service instance <i>id</i> ethernet</code>	イーサネット サービス インスタンスを定義し、イーサネット サービス コンフィギュレーション モードを開始します。

show ethernet service interface

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ついてのイーサネット カスタマー サービス インスタンスに関するインターフェイスベースの情報を表示するには、**show ethernet service interface** 特権 EXEC コマンドを使用します。

```
show ethernet service interface [interface-id] [detail] [| {begin | exclude | include}
expression]
```

構文の説明

<i>interface-id</i>	(任意) 指定したインターフェイスのサービスインスタンス情報を表示します。
detail	(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サービス インスタンスについての詳細情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 ethernet service interface** コマンドの出力を示します。

```
Switch# show ethernet service interface gigabitethernet0/1
Interface          Identifier
GigabitEthernet0/1 PE2-G101
```

```
Switch# show ethernet service interface detail
Interface: FastEthernet0/1
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/2
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/3
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
```

<output truncated>

```
Interface: GigabitEthernet0/1
ID: PE2-G101
CE-VLANS: 10,20,30
EVC Map Type: Bundling-Multiplexing
Associated EVCs:
EVC-ID CE-VLAN
WHITE 30
RED 20
BLUE 10
Associated Service Instances:
Service-Instance-ID CE-VLAN
10 10
20 20
30 30
```

関連コマンド

コマンド	説明
<code>service instance <i>id</i> ethernet</code>	イーサネット サービス インスタンスを定義し、インターフェイス コンフィギュレーション モードからイーサネット サービス コンフィギュレーション モードを開始します。

show facility-alarm relay major

指定されたリレー回路に関連付けられたファシリティ アラームを表示するには、**show facility-alarm relay major** ユーザ EXEC コマンドを使用します。

```
show facility-alarm relay major [ | {begin | exclude | include} expression]
```

構文の説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 facility-alarm relay minor** コマンドの出力を示します。マイナー リレーのアラーム情報が表示されます。

```
Switch> show facility-alarm relay minor
Source          Description                               Relay    Time
Switch          1 Temp above secondary thresh           MIN      Mar 01 1993 00:0 1:17
```

関連コマンド

コマンド	説明
alarm facility power-supply	電源アラーム オプションを設定します。
alarm facility temperature	温度アラーム オプションを設定します。
alarm profile (グローバル コンフィギュレーション)	インターフェイスに関連付けるアラーム ID とアラーム オプションが割り当てられたアラーム プロファイルを作成します。
show facility-alarm status	スイッチで生成されたアラームを表示します。

show facility-alarm status

スイッチで生成されたアラームをすべて表示するには、**show facility-alarm status** ユーザ EXEC コマンドを使用します。

```
show facility-alarm status [critical | info | major] [ | {begin | exclude | include}
expression]
```

構文の説明

critical	(任意) クリティカルなファシリティ アラームのみを表示します。
info	(任意) ファシリティ アラームをすべて表示します。
major	(任意) 主要なファシリティ アラーム以上をすべて表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 facility-alarm status** コマンドの出力を示します。スイッチのアラーム情報を表示します。

```
Switch> show facility-alarm status
Source          Severity Description          Relay    Time
FastEthernet1/3 MAJOR 2 Port Not Forwarding NONE     Mar 01
1993 00:02:22
```

関連コマンド

コマンド	説明
alarm facility power-supply	電源アラーム オプションを設定します。
alarm facility temperature	温度アラーム オプションを設定します。
alarm profile (グローバル コンフィギュレーション)	インターフェイスに関連付けるアラーム ID とアラーム オプションが割り当てられたアラーム プロファイルを作成します。
show facility-alarm relay major	スイッチで生成されたアラーム リレーを表示します。

show fcs-threshold

スイッチ インターフェイスのフレーム チェック シーケンス (FCS) ビットエラー レート設定を表示するには、**show fcs-threshold** ユーザ EXEC コマンドを使用します。

show fcs-threshold [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

イーサネット標準の上限ビット エラー レートは 10^{-8} です。Cisco CGS 2520 スイッチで設定可能なビット エラー レートの範囲は $10^{-6} \sim 10^{-11}$ です。ビット エラー レートをスイッチに入力するには、正の指数を使用します。出力では正の指数が表示されます。9 と出力された場合、ビット エラー レートは 10^{-9} 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 fcs-threshold** コマンドの出力を示します。ここでは、ポートがすべてデフォルトの FCS しきい値に設定された出力を示します。

```
Switch# show fcs-threshold
Port      FCS Threshold
Fa1/1      8
Fa1/2      8
Fa1/3      8
Fa1/4      8
Fa2/1      8
Fa2/2      8
Fa2/3      8
Fa2/4      8
Fa2/5      8
Fa2/6      8
Fa2/7      8
Fa2/8      8
Fa3/1      8
Fa3/2      8
Fa3/3      8
Fa3/4      8
Fa3/5      8
Fa3/6      8
Fa3/7      8
```

Fa3/8	8
Gi1/1	8
Gi1/2	8

関連コマンド

コマンド	説明
fcs-threshold	インターフェイスで FCS しきい値を設定します。

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 <i>interface-id</i>	(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 <i>number</i>	(任意) すべてのスイッチ上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。有効なモジュール番号は 1 のみです。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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。**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
-----
Gi0/1         Unsupp.  Unsupp.  off      off      0        0
Gi0/2         desired  off       off      off      0        0
Gi0/3         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 interface gigabitethernet0/2
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
-----
              admin    oper      admin    oper
-----
Gi0/2         desired off       off      off      0       0
```

関連コマンド

コマンド	説明
fcs-threshold	インターフェイスの受信フロー制御ステータスを設定します。

show idprom

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) 詳細な IDPROM 情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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、ギガビット イーサネット インターフェイスにのみ適用され、SFP モジュール スロットに挿入されている SFP についての情報を表示します。

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、ギガビット イーサネット インターフェイスの **show idprom interface** コマンドの出力を示します。

```
Switch# show idprom interface gigabitethernet0/1
```

```
General SFP Information
```

```
-----
Identifier          : 0x03
Connector           : 0x07
Transceiver         : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Encoding            : 0x02
BR_Nominal          : 0x01
Vendor Name         : CISCO-NEC
Vendor Part Number  : OD-BP1511-23SL2
Vendor Revision     : 0x30 0x30 0x30 0x31
Vendor Serial Number : NEC08440067
-----
```

Other Information

```
-----
Port asic num       : 0
Port asic port num  : 0
XCVR init completed : 1
Embedded PHY        : not present
SFP presence index  : 0
SFP iter cnt        : 697918
```

```
SFP failed oper flag : 0x0
IIC error cnt         : 0
IIC error dsb cnt    : 0
IIC max sts cnt      : 4
Chk for link status  : 1
Link Status           : 1
Link Status Media    : 1
Preferred media       : 0
Resolved Media       : 1
Config Media         : 1
Access Count         : 0
Access Count Max     : 2
Port Rx Loss         : no
Port Tx Fault        : no
Port Tx Disable      : no
```

Sfp selection asic reg map

```
-----
stbi                 : 0x00
sfpControl           : 0x4C
Regs Loc             : 0xF0000000
```

Page 0 Registers

```
-----
0000: 1140 Control Register           : 0001 0001 0100 0000
0001: 6149 Control STATUS             : 0110 0001 0100 1001
0002: 0141 Phy ID 1                   : 0000 0001 0100 0001
0003: 0C92 Phy ID 2                   : 0000 1100 1001 0010
0004: 01E1 Auto-Negotiation Advertisement : 0000 0001 1110 0001
0005: 0000 Auto-Negotiation Link Partner : 0000 0000 0000 0000
0006: 0004 Auto-Negotiation Expansion Reg : 0000 0000 0000 0100
0007: 2001 Next Page Transmit Register : 0010 0000 0000 0001
0008: 0000 Link Partner Next page Register : 0000 0000 0000 0000
0009: 0F00 1000BASE-T Control Register : 0000 1111 0000 0000
000A: 0000 1000BASE-T Status Register : 0000 0000 0000 0000
000F: 0000 Extended Status Register : 0000 0000 0000 0000
0010: 6028 PHY Specific Control Register : 0110 0000 0010 1000
0011: 6CC8 PHY Specific Status Register : 0110 1100 1100 1000
0012: 0000 Interrupt Enable Register : 0000 0000 0000 0000
0013: 0700 PHY Specific Status Register2 : 0000 0111 0000 0000
0015: 01C0 Receive Error Counter       : 0000 0001 1100 0000

0016: 0000 Page Address Register       : 0000 0000 0000 0000
001A: 8040 PHY Specific Control Register2 : 1000 0000 0100 0000
```

■ show idprom

関連コマンド

コマンド	説明
<code>show controllers ethernet-controller</code>	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 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 | rep | stats
| status [err-disabled] | switchport [backup | module number] | transceivers | trunk]
[ | {begin | exclude | include} expression]
```

構文の説明

<i>interface-id</i>	(任意) 有効なインターフェイスは、物理ポート（タイプ、モジュール、およびポート番号を含む）やポートチャネルなどです。ポートチャネル範囲は 1 ~ 48 です。
<i>vlan</i> <i>vlan-id</i>	(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 packets、オクテットを含む）を表示します。
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。
<i>module number</i>	(任意) スイッチ上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特性（上記のキーワードに対応）を表示します。有効なモジュール番号は 1 のみです。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。
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 スイッチ仮想インターフェイス（SVI）およびプライベート VLAN 混合ポートのプライベート VLAN マッピング情報を表示します。混合ポートは、ネットワークノードインターフェイス（NNI）である必要があります。キーワードは、スイッチでメトロアクセスイメージまたはメトロ IP アクセスイメージが稼動している場合にのみ表示されます。
rep	(任意) show interfaces rep コマンドを参照してください。
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 <i>unsupported</i> のステータスは、他社製の小型フォームファクタ（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) スイッチ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。キーワードは、スイッチでメトロアクセスイメージまたはメトロ IP アクセスイメージが稼動している場合にのみ表示されます。
transceivers	(任意) show interfaces transceivers コマンドを参照してください。

show interfaces

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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の文字列です。



(注)

crb、**fair-queue**、**irb**、**mac-accounting**、**precedence**、**pruning 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tring 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	変更箇所
12.2(53)EX	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 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。

- スイッチ上のすべてのインターフェイスの性能を表示するには、**show interfaces capabilities module 1** を使用します。これ以外の番号の入力は無効です。
- 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。
- スイッチ上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)。
- スイッチ上のすべてのインターフェイスのスイッチ ポート特性を表示するには、**show interface switchport module 1** を使用します。これ以外の番号の入力は無効です。

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、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 gigabitethernet0/2
GigabitEthernet0/2 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 interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
```

```

Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  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.

GigabitEthernet0/1
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/2
      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 gigabitethernet0/2 capabilities
GigabitEthernet0/2
Model:                                modell-ic
Type:                                  10/100/1000BaseTX SFP
Speed:                                 10,100,1000,auto
Duplex:                                half,full,auto
Trunk encap. type:                     802.1Q
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
SPAN:                                   source/destination
PortSecure:                             yes
Dot1x:                                  yes

```

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。

show interfaces

```
Switch# show interfaces gigabitethernet0/2 description
Interface Status          Protocol Description
Gi0/2          up              down      Connects to Marketing
```

次の例では、スイッチにポート チャン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、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
Port      Name              Status      Vlan      Duplex  Speed Type
Fa0/1     Fa0/1             connected   1         a-full  a-100 10/100BaseTX
Fa0/2     Fa0/2             connected   1         a-full  a-100 10/100BaseTX
Fa0/3     Fa0/3             notconnect  1         auto    auto  10/100BaseTX
Fa0/4     Fa0/4             disabled    1         auto    auto  10/100BaseTX
Fa0/5     Fa0/5             disabled    1         auto    auto  10/100BaseTX
Fa0/6     Fa0/6             disabled    1         auto    auto  10/100BaseTX
Fa0/7     Fa0/7             disabled    1         auto    auto  10/100BaseTX
Fa0/8     Fa0/8             disabled    1         auto    auto  10/100BaseTX
Fa0/9     Fa0/9             disabled    1         auto    auto  10/100BaseTX
Fa0/10    Fa0/10            disabled    1         auto    auto  10/100BaseTX
Fa0/11    Fa0/11            disabled    1         auto    auto  10/100BaseTX
Fa0/12    Fa0/12            disabled    1         auto    auto  10/100BaseTX
Fa0/13    Fa0/13            disabled    1         auto    auto  10/100BaseTX
Fa0/14    Fa0/14            disabled    1         auto    auto  10/100BaseTX
Fa0/15    Fa0/15            disabled    1         auto    auto  10/100BaseTX
```

```

Fa0/16                disabled    1          auto    auto 10/100BaseTX
Fa0/17                disabled    1          auto    auto 10/100BaseTX
Fa0/18                disabled    1          auto    auto 10/100BaseTX
Fa0/19                disabled    1          auto    auto 10/100BaseTX
Fa0/20                disabled    1          auto    auto 10/100BaseTX
Fa0/21                disabled    1          auto    auto 10/100BaseTX
Fa0/22                disabled    1          auto    auto 10/100BaseTX
Fa0/23                disabled    1          auto    auto 10/100BaseTX
Fa0/24                disabled    1          auto    auto 10/100BaseTX
Gi0/1                 notconnect 1          auto    auto 10/100/1000Ba
seTX SFP
Gi0/2                 connected  vl-err-dis a-full a-1000 10/100/1000BaseTX

```

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 22 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 fastethernet0/22 status
Port      Name          Status      Vlan      Duplex  Speed Type
Fa0/22    Fa0/22        connected   20,25     a-full  a-100 10/100BaseTX

```

次の例では、ポート 2 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 gigabitethernet0/2 status
Port      Name          Status      Vlan      Duplex  Speed Type
Gi0/2     Gi0/2         connected   20        a-full  a-100 10/100/1000BaseTX

```

次の例では、インターフェイスに対する **show interfaces status err-disabled** コマンドの出力を示します。

```

Switch# show interfaces gigabitethernet0/2 status err-disabled
Port      Name          Status      Reason          Err-disabled Vlans
Gi0/2     Gi0/2         connected   elmi evc down   1,200

```

次の例では、単一のポートの **show interfaces switchport** コマンドの出力を示します。表 2-14 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 gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
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 private VLANs: none
Operational private-vlan: none

```

show interfaces

```

Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Administrative Native VLAN tagging: enabled
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 private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

```

表 2-14 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	管理モードおよび動作モードを表示します。
Operational Mode	
Administrative Trunking Encapsulation	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。
Negotiation of Trunking	
Access Mode VLAN	ポートを設定する VLAN ID を表示します。
Trunking Native Mode VLAN	ネイティブ モードのトランクの VLAN ID を一覧表示します。
Administrative Native VLAN tagging	VLAN タギングがイネーブルになっているかどうかを表示します。
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。
Trunking VLANs enabled	トランク上のアクティブ VLAN を一覧表示します。
Capture VLANs allowed	トランク上の許可 VLAN を一覧表示します。
Unknown unicast 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。
Unknown multicast blocked	

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 interface gigabitethernet0/2 switchport
Name: Gi0/2
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
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、Flex Link インターフェイスがダウンして (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する場合の **show interfaces switchport backup** コマンドの出力を示します。この例では、インターフェイス Gi0/6 がダウンすると、Gi0/8 が Flex Link ペアのすべての VLAN を伝送します。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

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 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合は、G/0/8 が VLAN 60 および VLAN 100 ~ 120 のトラフィックを転送し、Gi0/6 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
-----
GigabitEthernet0/6    GigabitEthernet2/0/8  Active Up/Backup Up

Vlans on Interface Gi 0/6: 1-50
Vlans on Interface Gi 0/8: 60, 100-120
```

show interfaces

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 Gi0/6 がダウンすると、Gi0/8 が Flex Link ペアのすべての VLAN を伝送します。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

```
Vlans on Interface Gi 0/6:
Vlans on Interface Gi 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 Gi0/6 が再び稼働し始めると、このインターフェイスで優先される VLAN がピア インターフェイス Gi0/8 でブロックされ、Gi0/6 に転送されます。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet20/6	GigabitEthernet0/8	Active Up/Backup Up

```
Vlans on Interface Gi 0/6: 1-50
Vlans on Interface Gi 0/8: 60, 100-120
```

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 gigabitethernet0/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi0/1     auto     negotiate      trunking    1

Port      Vlans allowed on trunk
Gi0/1     1-4094

Port      Vlans allowed and active in management domain
Gi0/1     1-4

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     1-4
```

関連コマンド

コマンド	説明
switchport access vlan	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 メンバーシップ モードを設定します。

コマンド	説明
<code>switchport mode private-vlan</code>	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。
<code>switchport private-vlan</code>	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。

show interfaces counters

スイッチまたは指定されたインターフェイスの各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 | trunk] [module switch-
number] | etherchannel | protocol status] [| {begin | exclude | include} expression]
```

構文の説明

<i>interface-id</i>	(任意) 物理インターフェイスの ID (タイプ、モジュール、ポート番号を含む)。
errors	(任意) エラー カウンタを表示します。
trunk	(任意) トランク カウンタを表示します。
module switch- number	(任意) 指定されたスイッチ番号のカウンタを表示します。使用可能な値は 1 のみです。
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。
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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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tring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	変更箇所
12.2(53)EX	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
```

```

Fa0/1          0          0          0          0
Fa0/2          0          0          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
FastEthernet0/1: Other, IP, ARP, CDP
FastEthernet0/2: Other, IP
FastEthernet0/3: Other, IP
FastEthernet0/4: Other, IP
FastEthernet0/5: Other, IP
FastEthernet0/6: Other, IP
FastEthernet0/7: Other, IP
FastEthernet0/8: Other, IP
FastEthernet0/9: Other, IP
FastEthernet0/10: 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
Gi0/1          0              0              0
Gi0/2          0              0              0
Gi0/3        80678          4155           0
Gi0/4        82320          126            0
Gi0/5          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 interfaces rep

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ついての Resilient Ethernet Protocol (REP; レジリエントイーサネットプロトコル) 設定およびステータスを表示するには、**show interfaces rep** ユーザ EXEC コマンドを使用します。

```
show interfaces [interface-id] rep [detail] [| {begin | exclude | include} expression]
```

構文の説明

<i>interface-id</i>	(任意) 指定された物理インターフェイスまたはポート チャネル ID についての REP 設定およびステータスを表示します。
detail	(任意) 詳細な REP 設定およびステータス情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 interface rep [detail] コマンドの出力で、*Open*、*Fail*、または AP (代替ポート) ステートに加えて、Port Role に *Fail Logical Open (FailLogOpen)* または *Fail No Ext Neighbor (FailNoNbr)* と表示される場合があります。これらのステートは、ポートは物理的にアップしているが、ネイバーポートで REP が設定されていないことを示しています。この場合、設定中の接続性を維持するために、1つのポートがデータパスについてフォワーディングステートに移行します。このポートの Port Role は *Fail Logical Open* と表示され、ポートはすべての VLAN 上のすべてのデータトラフィックを転送します。障害が発生した別の Port Role には *Fail No Ext Neighbor* と表示され、このポートはすべての VLAN のトラフィックをブロックします。

障害が発生したポートのための外部ネイバーが設定されると、障害が発生したポートは代替ポート状態遷移を経て、代替ポート選択メカニズムに基づいて、最終的に *Open* ステートに移るか代替ポートのままになります。

show interfaces rep コマンドの出力では、エッジ、ネイバーなしに設定されているポートは *Primary Edge* または *Secondary Edge* の前にアスタリスク (*) で示されます。**show interfaces rep detail** コマンドの出力では、*No-Neighbor* と表示されます。

このコマンドの出力は **show tech-support** 特権 EXEC コマンドの出力にも含まれています。

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 interface rep** コマンドの出力を示します。

```
Switch # show interface rep
Interface                Seg-id  Type           LinkOp      Role
-----
GigabitEthernet 0/1      1       Primary Edge  TWO_WAY     Open
GigabitEthernet 0/2      1       Edge          TWO_WAY     Open
FastEthernet 0/4         2                     INIT_DOWN   Fail
```

次の例では、エッジポートに REP ネイバーがない構成の場合の **show interface rep** コマンドの出力を示します。*Primary Edge* の横にアスタリスク (*) が記されている点に注目してください。

```
Switch# show interface rep
Interface                Seg-id  Type           LinkOp      Role
-----
GigabitEthernet0/1      2       Primary Edge* TWO_WAY     Open
GigabitEthernet0/2      2       Primary Edge* TWO_WAY     Open
```

次の例では、外部ネイバーが設定されていないときの **show interface rep** コマンドの出力を示します。

```
Switch # show interface rep
Interface                Seg-id  Type           LinkOp      Role
-----
GigabitEthernet0/1      1       Primary Edge  NO_NEIGHBOR FailNoNbr
GigabitEthernet0/2      2       Primary Edge  NO_NEIGHBOR FailLogOpen
```

次の例では、指定されたインターフェイスについての **show interface rep detail** コマンドの出力を示します。

```
Switch # show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2  REP enabled
Segment-id: 1 (Segment)
PortID: 00030019E85BDD00
Preferred flag: No
Operational Link Status: INIT_DOWN
Current Key: 00000000000000000000
Port Role: Fail
Blocked VLAN: 1-4094
Admin-vlan: 1
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: 1234567890123456
Configured Load-balancing Block VLAN: 1-4094
STCN Propagate to: none
LSL PDU rx: 0, tx: 0
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

関連コマンド

コマンド	説明
rep segment	インターフェイス上で REP をイネーブルにし、セグメント ID を割り当てます。このコマンドは、ポートをエッジポート、プライマリエッジポート、または優先ポートとして設定するためにも使用されます。
show rep topology [detail]	プライマリエッジポートとして設定および選択されたポートを含む、セグメント内のすべてのポートに関する情報を表示します。

show interfaces transceivers

小型フォーム ファクタ (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するには、**show interfaces transceivers** 特権 EXEC コマンドを使用します。

show interfaces [*interface-id*] **transceiver** [**detail** | **module number** | **properties** | **supported-list** | **threshold-table**] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

<i>interface-id</i>	(任意) 物理インターフェイスの設定とステータスを表示します。
detail	(任意) (スイッチにインストールされている場合) Digital Optical Monitoring (DoM) 対応トランシーバの高低値やアラーム情報などの、調整プロパティを表示します。
supported-list	(任意) サポートされる DoM トランシーバをすべて表示します。
threshold-table	(任意) アラームおよび警告しきい値テーブルを表示します。 (注) このキーワードでは、SFP ハードウェアにプログラミングされているしきい値が表示されます。アラームまたはトラップを送信するタイミングを判断するためのしきい値は表示されません。これらのしきい値を表示するには、 show interfaces transceiver detail コマンドを入力します。
module number	(任意) スイッチのモジュールのインターフェイスへの表示を制限します。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。
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。
threshold-table	(任意) アラームおよび警告しきい値テーブルを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 interfaces transceiver threshold-table と **show interfaces transceiver detail** の出力に表示されるしきい値は、同じではありません。**show interfaces transceiver threshold-table** コマンドの出力に表示されるしきい値は Cisco IOS にハードコーディングされている値であり、サポートされていません。

show interfaces transceiver detail コマンドの出力に表示されるしきい値は SFP EEPROM から読み込まれ、サポートされます。トランシーバのしきい値を表示する場合は、常に **show interfaces transceiver detail** コマンドを使用する必要があります。

DOM しきい値は EEPROM からのパラメータがしきい値を超えた場合にトラップを送信するためのメカニズムを提供します。ファームウェアは、温度、電圧、送信電力および受信電力を含むリアルタイム値を SFP EEPROM から読み込み、これらの値を製品のアラームおよび警告しきい値と比較します。トランシーバトラップがイネーブルの場合にしきい値を超えると、トラップが 10 分ごとに送信されます。

CISCO-ENTITY-SENSOR-MIB での `entSensorThresholdTable` の読み取りおよびしきい値違反時の SNMP 通知は、Cisco IOS Release 12.2(52)SE 以降でのみサポートされています。

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 interface-id transceiver properties` コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet0/1 transceiver properties
Name : Gi0/1
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 gigabitethernet0/3 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.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi0/3	41.5	110.0	103.0	-8.0	-12.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi0/3	3.20	4.00	3.70	3.00	2.95

Port	Current (milliamperes)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi0/3	31.0	84.0	70.0	4.0	2.0

<output truncated>

次の例では、`show interfaces transceiver dom-supported-list` コマンドの出力を示します。

```
Switch# show interfaces transceiver dom-supported-list
Transceiver Type          Cisco p/n min version
                          supporting DOM
-----
DWDM GBIC                 ALL
DWDM SFP                  ALL
RX only WDM GBIC         ALL
DWDM XENPAK               ALL
```

show interfaces transceivers

```

DWDM X2                ALL
DWDM XFP               ALL
CWDM GBIC              NONE
CWDM X2                ALL
CWDM XFP               ALL
XENPAK ZR              ALL
X2 ZR                  ALL
XFP ZR                 ALL
Rx_only_WDM_XENPAK    ALL
XENPAK_ER              10-1888-03
X2_ER                  ALL
XFP_ER                 ALL
XENPAK_LR              10-1838-04
X2_LR                  ALL
<output truncated>

```

次の例では、**show interfaces transceiver threshold-table** コマンドの出力を示します。これらは IOS ソフトウェアにプログラムされたしきい値であり、アラームの決定に使用されないことに注意してください。

Optical Tx	Optical Rx	Temp	Laser Bias	Voltage current	

DWDM GBIC					
Min1	-0.50	-28.50	0	N/A	4.50
Min2	-0.30	-28.29	5	N/A	4.75
Max2	3.29	-6.69	60	N/A	5.25
Max1	3.50	6.00	70	N/A	5.50
DWDM SFP					
Min1	-0.50	-28.50	0	N/A	3.00
Min2	-0.30	-28.29	5	N/A	3.09
Max2	4.30	-9.50	60	N/A	3.59
Max1	4.50	9.30	70	N/A	3.70
RX only WDM GBIC					
Min1	N/A	-28.50	0	N/A	4.50
Min2	N/A	-28.29	5	N/A	4.75
Max2	N/A	-6.69	60	N/A	5.25
Max1	N/A	6.00	70	N/A	5.50
DWDM XENPAK					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
DWDM X2					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
DWDM XFP					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
CWDM X2					
Min1	N/A	N/A	0	N/A	N/A
Min2	N/A	N/A	0	N/A	N/A
Max2	N/A	N/A	0	N/A	N/A
Max1	N/A	N/A	0	N/A	N/A

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

ハードウェアの製品識別 (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

<i>entity-name</i>	(任意) 指定されたエンティティを表示します。たとえば、小型フォームファクタ (SFP) モジュールが取り付けられているインターフェイス (gigabitethernet 0/x など) を入力してその ID を表示します。
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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 ID を持つすべての識別可能なエンティティのコンパクト表示を生成します。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 PID、バージョン ID (VID)、シリアル番号 (SN) を含むそのエンティティの Unique Device Indicator (UDI) が表示されます。

多くのレガシー SFP には PID と VID がプログラミングされていません。



(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: "1", DESCR: "model-id"
PID: model-id , VID:Vol , SN: FSJC0407839

NAME: "GigabitEthernet0/1", DESCR: "100BaseBX-10U SFP"
PID: , VID: , SN: NEC08440067
NAME: "GigabitEthernet0/2", DESCR: "10/100/1000BaseTX SFP"
PID: , VID: , SN: 00000MTC0839048G
```

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タス、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せん。
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、Access Control List (ACL; アクセス コントロール リスト) 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タスを表示します。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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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
-----
Gi0/1     Untrusted   15          1
Gi0/2     Untrusted   15          1
Gi0/3     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 gigabitethernet0/1

Interface  Trust State  Rate (pps)  Burst Interval
-----
Gi0/1     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
-----
Gi0/1     5     0003.0000.d673  192.2.10.4    5         DHCP Deny   19:39:01 UTC
Mon Mar 1 1993
Gi0/1     5     0001.0000.d774  128.1.9.25    6         DHCP Deny   19:39:02 UTC
Mon Mar 1 1993
Gi0/1     5     0001.c940.1111  10.10.10.1    7         DHCP Deny   19:39:03 UTC
Mon Mar 1 1993
```

show ip arp inspection

```

Gi0/1      5      0001.c940.1112  10.10.10.2      8  DHCP Deny      19:39:04 UTC
Mon Mar 1 1993
Gi0/1      5      0001.c940.1114  173.1.1.1       10 DHCP Deny      19:39:06 UTC
Mon Mar 1 1993
Gi0/1      5      0001.c940.1115  173.1.1.2       11 DHCP Deny      19:39:07 UTC
Mon Mar 1 1993
Gi0/1      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タスを表示します。

```
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

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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
GigabitEthernet0/1      yes          unlimited
GigabitEthernet0/2      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

スイッチ上にあるすべてのインターフェイスの DHCP スヌーピング バインディング データベースと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

<i>ip-address</i>	(任意) バインディング エントリ IP アドレスを指定します。
<i>mac-address</i>	(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 <i>interface-id</i>	(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 <i>vlan-id</i>	(任意) バインディング エントリ VLAN を指定します。
begin	<i>expression</i> と一致する行から表示を開始します。
exclude	<i>expression</i> と一致する行を表示から除外します。
include	指定した <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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    GigabitEthernet0/1
00:D0:B7:1B:35:DE  10.1.2.151    237        dhcp-snooping  20    GigabitEthernet0/2
Total number of bindings: 2
```

■ show ip dhcp snooping binding

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      GigabitEthernet0/1
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      GigabitEthernet0/2
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 gigabitethernet0/2
-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN    Interface
-----
00:30:94:C2:EF:35  10.1.2.151    290           dhcp-snooping  20      GigabitEthernet0/2
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      GigabitEthernet0/1
00:00:00:00:00:02  10.1.2.151    65            dhcp-snooping  20      GigabitEthernet0/2
Total number of bindings: 2
```

表 2-15 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 2-15 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :          0   Startup Failures :          0
Successful Transfers :          0   Failed Transfers :          0
Successful Reads     :          0   Failed Reads      :          0
Successful Writes    :          0   Failed Writes     :          0
Media Failures       :          0
```

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
```

■ show ip dhcp snooping database

```

Last Succeeded 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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 2-16 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 2-16 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。

表 2-16 DHCP スヌーピング統計情報

DHCP スヌーピング統計情報	説明
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。
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

<i>profile number</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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] [detail]] [vlan vlan-id]
[detail] [| {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 <i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。

出力に表示される Source-Only ラーニングの行は無効です。

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 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
```

show ip igmp snooping

```
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
```



(注)

Source-Only ラーニングはサポートされていないため、この機能について表示される情報は無効です。

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	スイッチ上または VLAN 上の IGMP スヌーピングをイネーブルにし、設定を行います。
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 テーブルを表示するか、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-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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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。

show ip igmp snooping groups

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
-----
104       224.1.4.2  igmp     v2        Gi0/1, Gi0/2
104       224.1.4.3  igmp     v2        Gi0/1, Gi0/2
```

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        Gi0/1, Fa0/15
104       224.1.4.3  igmp     v2        Gi0/1, Fa0/15
```

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        Gi0/1, Fa0/15
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチ上または VLAN 上の IGMP スヌーピングをイネーブルにし、設定を行います。
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 に対して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

<code>vlan <i>vlan-id</i></code>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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         Gi0/1 (dynamic)
```

■ show ip igmp snooping mrouter

関連コマンド

コマンド	説明
ip igmp snooping	スイッチ上または VLAN 上の IGMP スヌーピングをイネーブルにし、設定を行います。
ip igmp snooping vlan mrouter	マルチキャストの VLAN にマルチキャスト ルータ ポートを追加します。
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

最後にスイッチが受信したインターネットグループ管理プロトコル (IGMP) クエリーの IP アドレスおよび着信ポートを表示するには、`show ip igmp snooping querier` ユーザ EXEC コマンドを使用します。

```
show ip igmp snooping querier [vlan vlan-id] [detail] [ | {begin | exclude | include}
expression]
```

構文の説明

<code>vlan <i>vlan-id</i></code>	(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。
<code>detail</code>	(任意) クエリアに関してクエリア情報、設定および動作情報を表示します。
<code> begin</code>	(任意) <i>expression</i> と一致する行から表示を開始します。
<code> exclude</code>	(任意) <i>expression</i> と一致する行を表示から除外します。
<code> include</code>	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<code><i>expression</i></code>	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	変更箇所
12.2(53)EX	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 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。

■ show ip igmp snooping querier

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                 Gi0/1
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                 Fa0/1

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 Fa0/1
-----
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 querier	スイッチ上または VLAN 上の IGMP スヌーピング クェリアをイネーブルにし、設定を行います。
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 sla standards

スイッチに実装されている Cisco IOS IP サービス レベル契約 (SLA) および双方向アクティブ測定プロトコル (TWAMP) 標準を表示するには、**show ip sla standards** コマンドをユーザ EXEC モードまたは特権 EXEC モードで使用します。

show ip sla standards

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

スイッチ上に実装されている IP SLA および TWAMP 標準を表示します。

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スイッチ上に実装されている IP SLA TWAMP 標準を表示するには、**show ip sla standards** コマンドを使用します。

例

次の例では、**show ip sla standards** コマンドの出力を示します。

```
Switch> show ip sla standards
Feature           Organization      Standard
TWAMP Server      IETF              draft-ietf-ippm-twamp-06
TWAMP Reflector   IETF              draft-ietf-ippm-twamp-06
```

関連コマンド

コマンド	説明
show ip sla twamp connection {detail requests}	IP SLA TWAMP 接続を表示します。
show ip sla twamp session	IP SLA TWAMP セッションを表示します。

show ip sla twamp connection

現在の Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) 接続を表示するには、**show ip sla twamp connection** コマンドをユーザ EXEC モードで使用します。

```
show ip sla twamp connection {detail [source-ip ip-address] | requests} [| {begin |
exclude | include} expression]
```

構文の説明

detail	現在の接続の詳細を表示します。
source-ip ip-address	(任意) 特定の TWAMP 接続による接続詳細を表示します。
requests	現在の接続要求を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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

実行中のすべての IP SLA TWAMP セッションの出力を表示します。

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

単一の IP SLA TWAMP 接続の詳細情報を表示するには、**detail** キーワードを使用します。

現在の IP SLA TWAMP 接続要求を表示するには、**requests** キーワードを使用します。

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 sla twamp connection detail** コマンドの出力を示します。

```
Switch> show ip sla twamp connection detail
Connection Id:          91
  Client IP Address:    172.27.111.225
  Client Port:         43026
  Mode:                Unauthenticated
  Connection State:    Connected
  Control State:       None
  Number of Test Requests - 0:1
```

次の例では、**show ip sla twamp connection requests** コマンドの出力を示します。

```
Switch> show ip sla twamp connection requests
Connection-Id      Client Address    Client Port
          91      172.27.111.225    43026
Total number of current connections: 1
```

関連コマンド

コマンド	説明
show ip sla standards	スイッチ上に実装されている TWAMP サーバおよびリフレクタ標準を表示します。
show ip sla twamp session	IP SLA TWAMP セッションを表示します。

show ip sla twamp session

Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) テストセッションを表示するには、**show ip sla twamp session** コマンドをユーザ EXEC モードで使用します。

```
show ip sla twamp session [source-ip ip address | source-port port-number] [| {begin |
exclude | include} expression]
```

構文の説明

source-ip <i>ip-address</i>	(任意) 指定された IP アドレスでの TWAMP テストセッションの結果を表示します。
source-port <i>port-number</i>	(任意) 指定されたポートでの TWAMP テストセッションの結果を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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

IP SLA TWAMP テストセッションおよび結果を表示します。

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	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 SLA TWAMP テストセッションに関する情報を表示するには、**show ip sla twamp session** 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 sla twamp session** コマンドの出力を示します。

```
Switch> show ip sla twamp session
IP SLAs Responder TWAMP is: Enabled
Recv Addr: 172.27.117.116
Recv Port: 3619
Sender Addr: 172.27.111.225
Sender Port: 32910
Session Id: 172.27.117.116:533112:9C41EC42
Connection Id: 95
```

関連コマンド

コマンド	説明
show ip sla standards	スイッチ上に実装されている TWAMP サーバおよびリフレクタ標準を表示します。
show ip sla twamp connection {detail requests}	IP SLA TWAMP 接続を表示します。

show ip source binding

スイッチ上の IP ソース 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**] [**vlan** *vlan-id*]
[**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

<i>ip-address</i>	(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。
<i>mac-address</i>	(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。
vlan <i>vlan-id</i>	(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。
interface <i>interface-id</i>	(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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。

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    GigabitEthernet0/1
00:00:00:0A:00:0A  11.0.0.2      10000       dhcp-snooping  10    GigabitEthernet0/1
```

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

スイッチまたは特定のインターフェイス上の IP ソース ガード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	変更箇所
	12.2(53)EX	このコマンドが追加されました。

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
-----  -
fa0/1     ip           active       10.0.0.1        -----
fa0/1     ip           active       deny-all       11-20
fa0/2     ip           inactive-trust-port
fa0/3     ip           inactive-no-snooping-vlan
fa0/4     ip-mac       active       10.0.0.2        aaaa.bbbb.cccc  10
fa0/4     ip-mac       active       11.0.0.1        aaaa.bbbb.cccd  11
fa0/4     ip-mac       active       deny-all       deny-all        12-20
fa0/5     ip-mac       active       10.0.0.3        permit-all      10
fa0/5     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。

- ファストイーサネット 0/1 インターフェイスでは、動的ホスト制御プロトコル (DHCP) スヌーピングは VLAN 10 ~ 20 上でイネーブルになります。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 番目のエントリに、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に対してデフォルト ポート Access Control List (ACL; アクセス コントロール リスト) が適用されていることが示されています。
- ファストイーサネット 0/2 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。
- ファストイーサネット 0/3 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。

■ show ip verify source

- ファストイーサネット 0/4 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は、VLAN 10 および 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。
- ファストイーサネット 0/5 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 gigabitethernet0/6  
IP source guard is not configured on the interface gi0/6.
```

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

プロセス間通信 (IPC) 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 [cumulative] | 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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 [cumulative]	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。 <ul style="list-style-type: none"> • cumulative : (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 個の IPC ゾーンをサポートします。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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

■ show ipc

コマンド履歴

リリース	変更箇所
12.2(53)EX	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、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 Sent	Last 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 msgns 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 msgns 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
```

■ show ipc

```
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	変更箇所
12.2(53)EX	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 {default | routing | 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。

例

次の例では、**show ipv6 access-list** コマンドで出力された *inbound* という名前の IPv6 アクセス リストを示します。

```
Switch# 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 2-17 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 2-17 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。構文情報については、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5845/products_command_reference_chapter09186a008027e846.html#wp1238563
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、スイッチでメトロ IP アクセス イメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できません。

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。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	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 | routing | 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。クライアントはネイバー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、そのアドレスはプールから削除され、競合リストから削除されるまでこのアドレスを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 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、**show ipv6 route updated** ユーザ EXEC 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

<i>protocol</i>	(任意) 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。次のいずれかのキーワードを入力できます。 <ul style="list-style-type: none"> • eigrp • ospf • rip または指定したルート タイプのルートを表示します 次のいずれかのキーワードを入力できます。 <ul style="list-style-type: none"> • connected • local • static • interface <i>interface id</i>
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。
<i>hh:mm</i>	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。
<i>day</i>	日にちを入力します。指定できる範囲は 1 ~ 31 です。
<i>month</i>	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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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, GigabitEthernet0/1
Last updated 10:31:10 27 February 2007
R 2004::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/2
Last updated 17:23:05 22 February 2007
R 4000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/3
Last updated 17:23:05 22 February 2007
R 5000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/4
Last updated 17:23:05 22 February 2007
R 5001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/5
Last updated 17:23:05 22 February 2008
```

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。構文情報については、「Cisco IOS Software」> 「Command References for the Cisco IOS Software Releases 12.3 Mainline」> 『Cisco IOS IPv6 Command Reference』> 「IPv6 Commands: show ipv6 nat translations through show ipv6 protocols」を選択してください。

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 ~ 64 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 ポート、トランク ポート、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 Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Fa0/3	---	----	----	----	----	----
	pagp	----	----	0	242500	
	lACP	----	----	24268	242640	
	udld	----	----	0	897960	
Fa0/4	---	----	----	----	----	----
	pagp	1000	----	24249	242700	
	lACP	----	----	24256	242660	
	udld	----	----	0	897960	
Gi0/1	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	pagp	1000	----	0	242500	
	lACP	500	----	0	485320	
	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 Threshold (cdp/stp/vtp) (pagp/lACP/udld)	Drop Threshold (cdp/stp/vtp) (pagp/lACP/udld)	Status
Fa0/2	pagp lACP udld	----/----/----	----/----/----	up
Fa0/3	pagp lACP udld	1000/----/----	----/----/----	up
Fa0/4	pagp lACP udld	1000/ 500/----	----/----/----	up
Fa0/5	cdp stp vtp	----/----/----	----/----/----	down
Gi0/1	pagp	----/----/----	1000/----/----	down
Gi0/2	pagp	----/----/----	1000/----/----	down

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 Class of Service (CoS; サービス クラス) 値を設定します。

show lacp

Link Aggregation Control Protocol (LACP) チャンネル 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]
```



(注)

LACP を使用できるのは、ネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) 上だけです。

構文の説明

<i>channel-group-number</i>	(任意) チャンネル 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 lacp コマンドを入力すると、アクティブなチャンネル グループの情報が表示されます。特定のチャンネル情報を表示するには、チャンネル グループ番号を指定して **show lacp** コマンドを入力します。

チャンネル グループを指定しない場合は、すべてのチャンネル グループが表示されます。

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ンネル 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 2-18 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
          LACPDU          Marker      Marker Response      LACPDU
Port      Sent   Recv      Sent   Recv      Sent   Recv      Pkts Err
-----
Channel group:1
Gi0/1      19    10         0     0         0     0         0
Gi0/2      14     6         0     0         0     0         0
```

表 2-18 show lacp counters のフィールドの説明

フィールド	説明
LACPDU 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
LACPDU 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 LACPDU
       F - Device is requesting Fast LACPDU
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1

Port      Flags  State      LACP port  Admin  Oper  Port  Port
Gi0/1     SA     bndl      32768      0x3    0x3   0x4   0x3D
Gi0/2     SA     bndl      32768      0x3    0x3   0x5   0x3D
```

表 2-19 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 2-19 show lacp internal のフィールドの説明

フィールド	説明
State	<p>特定のポートの状態。次に使用可能な値を示します。</p> <ul style="list-style-type: none"> - : 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 : ポートを他の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	<p>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。</p>

show lacp

表 2-19 show lacp internal のフィールドの説明 (続き)

フィールド	説明
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せん (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。
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せん (16 進数)。
Port Number	ポート番号。
Port State	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>(注) 上のリストでは、bit7 が MSB で bit0 は LSB です。</p>

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:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi0/1	32768,0007.eb49.5e80	0xC	19s	SP
	LACP Partner	Partner	Partner	
	Port Priority	Oper Key	Port State	
	32768	0x3	0x3C	

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi0/2	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 チャンネル 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 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** 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。

```
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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 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 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 : Gi0/15(Dwn) Gi0/16(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn) Gi0/17(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

show lldp

show lldp コマンドについては、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_04.html#wp1095571.

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	Emergency Location Information (ELIN; 緊急ロケーション情報) 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 gigabitethernet2/0/1
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 logging onboard

オンボード障害ロギング (OBFL) 情報を表示するには、**show logging onboard** 特権 EXEC コマンドを使用します。

```
show logging onboard [module [slot-number]] {{clilog | environment | message
|temperature | uptime | voltage} [continuous | detail | summary] [start hh:mm:ss day
month year] [end hh:mm:ss day month year]} [| {begin | exclude | include} expression]
```

構文の説明

module [slot-number]	(任意) module スロット番号は常に 1 で、CGS 2520 には関連しません。
clilog	スイッチ上に入力された OBFL CLI コマンドを表示します。
environment	製品 ID (PID)、バージョン ID (VID)、シリアル番号など、スイッチおよびすべての接続デバイスに関する Unique Device Identifier (UDI) 情報を表示します。
message	スイッチによって生成されたハードウェア関連のシステム メッセージを表示します。
temperature	スイッチの温度を表示します。
uptime	スイッチが起動する時間、スイッチが再起動する理由、最後に再起動して以降スイッチが稼動している時間を表示します。
voltage	スイッチのシステム電圧を表示します。
continuous	(任意) 連続ファイルのデータを表示します。詳細については、「使用上のガイドライン」を参照してください。
summary	(任意) サマリーファイルのデータを表示します。詳細については、「使用上のガイドライン」を参照してください。
start hh:mm:ss day month year	(任意) 指定した日時からのデータを表示します。詳細については、「使用上のガイドライン」を参照してください。
end hh:mm:ss day month year	(任意) 指定した日時までのデータを表示します。詳細については、「使用上のガイドライン」を参照してください。
detail	(任意) 連続データおよびサマリー データの両方を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

OBFL がイネーブルの場合、スイッチは循環式の連続ファイルにすべての OBFL データを記録します。連続ファイルがいっぱいになると、スイッチはサマリーファイル（別名、履歴ファイル）にデータをまとめます。スイッチは、連続ファイルに新しいデータを書き込み続けます。

特定の時間内にだけ収集されたデータを表示するには、**start** キーワードと **end** キーワードを使用します。**start** 時刻および **end** 時刻を指定するときには、次の注意事項に従ってください。

- **hh:mm:ss** : 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、**13:32:45** 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。
- **year** : 4 桁の数字で年を入力します（例：2008）。指定できる範囲は 1993 ~ 2035 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 logging onboard cliilog continuous** コマンドの出力を示します。

```
Switch# show logging onboard cliilog continuous
-----
CLI LOGGING CONTINUOUS INFORMATION
-----
MM/DD/YYYY HH:MM:SS COMMAND
-----
05/12/2006 15:33:17 show logging onboard temperature detail
05/12/2006 15:33:21 show logging onboard voltage detail
05/12/2006 16:14:09 show logging onboard temperature summary
...
<output truncated>
....
05/16/2006 13:07:53 no hw-module module logging onboard message level
05/16/2006 13:16:13 show logging onboard uptime continuous
05/16/2006 13:39:18 show logging onboard uptime summary
05/16/2006 13:45:57 show logging onboard cliilog summary
-----
```

次の例では、**show logging onboard message** コマンドの出力を示します。

```
Switch# show logging onboard message
-----
ERROR MESSAGE SUMMARY INFORMATION
-----
Facility-Sev-Name      | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
-----
No historical data to display
-----
```

show logging onboard

次の例では、**show logging onboard status** コマンドの出力を示します。

```
Switch# show logging onboard status
Devices registered with infra
      Slot no.: 0 Subslot no.: 0, Device obf10:
Application name cilog :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name environment :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name errmsg :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name poe :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name temperature :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name uptime :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
Application name voltage :
      Path : obf10:
      CLI enable status : enabled
      Platform enable status: enabled
```

次の例では、**show logging onboard temperature continuous** コマンドの出力を示します。

```
Switch# show logging onboard temperature continuous
-----
TEMPERATURE CONTINUOUS INFORMATION
-----
Sensor | ID |
-----
Board temperature | 1 |
-----

Time Stamp |Sensor Temperature OC
MM/DD/YYYY HH:MM:SS | 1 2 3 4 5 6 7 8 9 10 11 12
-----
05/12/2006 15:33:20 | 35 -- -- -- -- -- -- -- -- -- --
05/12/2006 16:31:21 | 35 -- -- -- -- -- -- -- -- -- --
05/12/2006 17:31:21 | 35 -- -- -- -- -- -- -- -- -- --
05/12/2006 18:31:21 | 35 -- -- -- -- -- -- -- -- -- --
05/12/2006 19:31:21 | 35 -- -- -- -- -- -- -- -- -- --
05/12/2006 20:31:21 | 35 -- -- -- -- -- -- -- -- -- --
05/12/2006 21:29:22 | 35 -- -- -- -- -- -- -- -- -- --
05/12/2006 22:29:22 | 35 -- -- -- -- -- -- -- -- -- --
05/12/2006 23:29:22 | 35 -- -- -- -- -- -- -- -- -- --
05/13/2006 00:29:22 | 35 -- -- -- -- -- -- -- -- -- --
05/13/2006 01:29:22 | 35 -- -- -- -- -- -- -- -- -- --
05/13/2006 02:27:23 | 35 -- -- -- -- -- -- -- -- -- --
05/13/2006 03:27:23 | 35 -- -- -- -- -- -- -- -- -- --
05/13/2006 04:27:23 | 35 -- -- -- -- -- -- -- -- -- --
05/13/2006 05:27:23 | 35 -- -- -- -- -- -- -- -- -- --
05/13/2006 06:27:23 | 35 -- -- -- -- -- -- -- -- -- --
```

```
05/13/2006 07:25:24 36 -- -- -- -- -- -- -- -- --
05/13/2006 08:25:24 35 -- -- -- -- -- -- -- -- --
<output truncated>
```

次の例では、**show logging onboard uptime summary** コマンドの出力を示します。

```
Switch# show logging onboard uptime summary
-----
UPTIME SUMMARY INFORMATION
-----
First customer power on : 03/01/1993 00:03:50
Total uptime           : 0 years 0 weeks 3 days 21 hours 55 minutes
Total downtime        : 0 years 0 weeks 0 days 0 hours 0 minutes
Number of resets       : 2
Number of slot changes : 1
Current reset reason   : 0x0
Current reset timestamp: 03/01/1993 00:03:28
Current slot           : 1
Current uptime         : 0 years 0 weeks 0 days 0 hours 55 minutes
-----
Reset |      |
Reason | Count |
-----
No historical data to display
-----
```

次の例では、**show logging onboard voltage summary** コマンドの出力を示します。

```
Switch# show logging onboard voltage summary
-----
VOLTAGE SUMMARY INFORMATION
-----
Number of sensors       : 8
Sampling frequency     : 60 seconds
Maximum time of storage : 3600 minutes
-----
Sensor                  | ID | Maximum Voltage
-----
12.00V                  | 0  | 12.567
5.00V                   | 1  | 5.198
3.30V                   | 2  | 3.439
2.50V                   | 3  | 2.594
1.50V                   | 4  | 1.556
1.20V                   | 5  | 1.239
1.00V                   | 6  | 0.980
0.75V                   | 7  | 0.768
-----
Nominal Range           | Sensor ID
-----
No historical data to display
-----
```

関連コマンド

コマンド	説明
clear logging onboard	フラッシュ メモリ内の OBFL データを削除します。
hw-module module logging onboard	OBFL をイネーブルにします。

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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。この表示では、ファストイーサネット インターフェイス 0/2 で着信トラフィックに MAC アクセス リスト *macl_e1* が適用されています。他のインターフェイスには MAC ACL が適用されていません。

```
Switch> show mac access-group
Interface FastEthernet0/1:
  Inbound access-list is macl_e1
  Outbound access-list is not set
Interface FastEthernet0/2:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/3:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/4:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernetv0/5:
  Inbound access-list is not set
  Outbound access-list is not set
<output truncated>
```

次の例では、**show mac access-group interface fastethernet0/1** コマンドの出力を示します。

```
Switch# show mac access-group interface fastethernet0/1
Interface FastEthernet0/1:
  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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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** 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 Gi0/4
Total Mac Addresses for this criterion: 12
```

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 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

指定した 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

<i>mac-address</i>	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 <i>interface-id</i>	(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 チャンネルが含まれます。
vlan <i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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 インスタンスのエイジング 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 インスタンスのエイジング 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 <i>vlan-id</i>	(任意) 特定の VLAN のエイジング 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 番号が指定されない場合、すべての VLAN に対するエイジング 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 <i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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。
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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 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 Gi0/2
1       00b0.6496.2741   DYNAMIC Gi0/2
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

<i>interface-id</i>	(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 <i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 interface** コマンドの出力を示します。

```
Switch> show mac address-table interface gigabitethernet0/2
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
  1     0030.b635.7862   DYNAMIC Gi0/2
  1     00b0.6496.2741   DYNAMIC Gi0/2
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 ラーニング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

コマンド モード ユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	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 ラーニング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 ラーニングがイネーブルです。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 ラーニングが 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 ラーニング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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
	12.2(53)EX	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#
```

■ show mac address-table move update

関連コマンド

コマンド	説明
<code>clear mac address-table move update</code>	MAC アドレス テーブル移行更新カウンタをクリアします。
<code>mac address-table move update {receive transmit}</code>	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。
<i>interface-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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
```

show mac address-table notification

```

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。
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 <i>mac-address</i>	(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 <i>interface-id</i>	(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 チャンネルが含まれます。
vlan <i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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	
<i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
	12.2(53)EX	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 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 monitor

スイッチ上のすべてのスイッチドポートアナライザ (SPAN) セッションおよびリモート SPAN (RSPAN) セッションの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。
<i>session_number</i>	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 (<i>list</i> 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せん)。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	<i>expression</i> と一致する行から表示を開始します。
exclude	<i>expression</i> と一致する行を表示から除外します。
include	指定した <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。

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:      Fa0/24
  TX Only:      None
  Both:         Fa0/1-2,Fa0/1-5
Destination Ports:Fa0/18
  Encapsulation:Replicate

Session 2
-----
Type           :Remote Source Session
Source Ports:
Source VLANs:
TX Only:       10
  Both:        1-9
Dest RSPAN VLAN: 105
```

次に、RSPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力例を示します。

```
Switch# show monitor session 1
Session 1
-----
Type           :Local Session
Source Ports:
  RX Only:      Fa0/24
  TX Only:      None
  Both:         Fa0/1-2,Fa0/1-5
Destination Ports:Fa0/18
  Encapsulation:Replicate
```

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         :Fa0/2
Destination Ports :Fa0/3
  Encapsulation :Replicate
  Ingress:Enabled, default VLAN = 5
  Ingress encapsulation:DOT1Q

Session 2
-----
Type           :Local Session
Source Ports   :
  Both         :Fa0/1
Destination Ports :Fa0/4
  Encapsulation :Replicate
  Ingress:Enabled
  Ingress encapsulation:DOT1Q
```

関連コマンド

コマンド	説明
<code>monitor session</code>	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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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)	スイッチ上でマルチキャスト VLAN レジストレーション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 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

<i>interface-id</i>	(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。 有効なインターフェイスは物理ポート (タイプ、モジュール、ポート番号を含む) を含みます。
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 <i>vlan-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。

show mvr interface *interface-id* コマンドを入力し、指定されたポートが非 MVR ポートの場合、出力の Type フィールドには NON MVR と表示されます。アクティブな MVR ポートの場合、ポートタイプ (RECEIVER または SOURCE)、モード (アクセスまたはトランク)、VLAN、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。

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           Mode           VLAN    Status           Immediate Leave
----      -
Fa0/1     Receiver       Trunk          1       ACTIVE/UP        DISABLED
Fa0/1     Receiver       Trunk          2000    ACTIVE/DOWN      DISABLED
Fa0/2     Receiver       Trunk          2       ACTIVE/UP        DISABLED
Fa0/2     Receiver       Trunk          3000    ACTIVE/UP        DISABLED
Fa0/3     Receiver       Trunk          2       ACTIVE/UP        DISABLED
Fa0/3     Receiver       Trunk          3000    ACTIVE/UP        DISABLED
Fa0/10    Source         Access         10      ACTIVE/UP        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、**show mvr interface fastethernet0/10** コマンドの出力を示します。

```
switch# show mvr interface fa0/10
Port      Type           Mode           VLAN    Status           Immediate Leave
----      -
Fa0/10    RECEIVER       Trunk          201     ACTIVE/DOWN      DISABLED
```

次の例では、**show mvr interface fastethernet0/1** コマンドの出力を示します。この例では、ポートは MVR のメンバになっていません。

```
switch# show mvr interface fa0/1
Port      Type           Mode           VLAN    Status           Immediate Leave
----      -
Fa0/1     NON MVR        Access         0       INACTIVE         DISABLED
```

次の例では、**show mvr interface gigabitethernet0/1 members** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet0/1 members
239.255.0.0   vlan 202    DYNAMIC ACTIVE
239.255.0.1   vlan 202    DYNAMIC ACTIVE
239.255.0.2   vlan 202    DYNAMIC ACTIVE
239.255.0.3   vlan 203    DYNAMIC ACTIVE
239.255.0.4   vlan 203    DYNAMIC ACTIVE
239.255.0.5   vlan 203    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)	スイッチ上でマルチキャスト VLAN レジストレーション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メンバー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

<i>ip-address</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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      Status      Members    VLAN    Membership
-----
239.1.1.1      ACTIVE     Fa0/1      1       Static
239.1.1.1      ACTIVE     Fa0/1      2000    Static
239.1.1.1      ACTIVE     Fa0/2      2       Static
239.1.1.1      ACTIVE     Fa0/2      3000    Static
239.1.1.2      ACTIVE     Fa0/1      1       Static
239.1.1.2      ACTIVE     Fa0/2      2       Static
```

<output truncated>

次の例では、**show mvr members 239.255.0.2** コマンドの出力を示します。IP マルチキャスト グループ 239.255.0.2 のメンバを表示する例を示します。

```
Switch# show mvr members 239.255.0.2
239.255.0.2      ACTIVE          Gi0/1 (d), Gi0/2 (d), Gi0/3 (d),
                  Gi0/4 (d), Gi0/5 (s)
```

関連コマンド

コマンド	説明
<code>mvr</code> (グローバル コンフィギュレーション)	スイッチ上でマルチキャスト VLAN レジストレーションをイネーブルにして、設定します。
<code>mvr</code> (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。
<code>show mvr</code>	スイッチのグローバル MVR 設定を表示します。
<code>show mvr interface</code>	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 pagp

ポート集約プロトコル (PAgP) チャンネル 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 | internal | neighbor} [| {begin | exclude | include} expression]]
```



(注)

PAgP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

構文の説明

<i>channel-group-number</i>	(任意) チャンネル 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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 pagp コマンドを入力すると、アクティブなチャンネル グループの情報が表示されます。非アクティブ ポート チャンネルの情報を表示するには、チャンネル 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
Gi0/1     45    42         0      0
Gi0/2     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

Port      Flags State  Timers Interval Hello Partner PAgP Learning Group
Gi0/1     SC   U6/S7  H      30s      1       1    128   Any    16
Gi0/2     SC   U6/S7  H      30s      1       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

Port      Partner Name      Partner Device ID      Partner Port      Age  Flags  Cap.
Gi0/1     switch-p2  0002.4b29.4600  Gi0/1          9s  SC    10001
Gi0/2     switch-p2  0002.4b29.4600  Gi0/2          24s SC    10001
```

関連コマンド

コマンド	説明
clear pagp	PAGP チャンネル グループ情報をクリアします。

show parser macro

スイッチ上のすべての設定済みマクロまたは 1 つのマクロのパラメータを表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。

```
show parser macro [{brief | description [interface interface-id] | name macro-name}]
                  [| {begin | exclude | include} expression]
```

構文の説明

brief	(任意) 各マクロの名前を表示します。
description [interface interface-id]	(任意) すべてのマクロの説明または特定のインターフェイスの説明を表示します。
name macro-name	(任意) マクロ名で特定された 1 つのマクロに関する情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 parser macro** コマンドの出力を示します。

```
Switch# show parser macro
Total number of macros = 2
-----
Macro name : sample-macrol
Macro type : customizable
duplex full
speed auto
mdix auto
-----
Macro name : test1
Macro type : customizable
no shutdown
flowcontrol receive on
speed 100
-----
```

次の例では、**show parser macro name** コマンドの出力を示します。

```
Switch# show parser macro name sample-macro1
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
```

次の例では、**show parser macro brief** コマンドの出力を示します。

```
Switch# show parser macro brief
customizable      : sample-macro1
customizable      : test1
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	インターフェイスに適用されたマクロについての説明を追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
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 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

show policer aggregate

すべての集約ポリサーまたは特定のポリサーの Quality of Service (QoS) 集約ポリサー情報を表示するには **show policer aggregate** ユーザ EXEC コマンドを使用します。

```
show policer aggregate [aggregate-policer-name] [ | {begin | exclude | include}
expression]
```

構文の説明

<i>aggregate-policer-name</i>	(任意) 集約ポリサーの名前。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 policer aggregate** コマンドの出力を示します。

```
Switch> show policer aggregate my-policer
aggregate-policer: my-policer

    police cir 12000000 bc 5000
      conform-action transmit
      exceed-action set-cos-transmit cos table 67577

In use by policymap: pin
```

関連コマンド

コマンド	説明
police aggregate (ポリシーマップ クラス コンフィギュレーション)	同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。
policer aggregate (グローバル コンフィギュレーション)	インターフェイスで受信されるすべてのトラフィックをポリシングする集約ポリサーを作成します。

show policer cpu uni-eni

スイッチ上に設定されているコントロール プレーンのセキュリティ機能でのドロップされたフレーム数やしきい値レートを含む、スイッチのユーザ ネットワーク インターフェイス (UNI) および拡張 ネットワーク インターフェイス (ENI) のコントロール プレーン ポリサー情報を表示するには、**show policer cpu uni-eni** ユーザ EXEC コマンドを使用します。

```
show policer cpu uni-eni {drop [interface interface-id]] | rate} [| {begin | exclude | include} expression]
```

構文の説明

drop	(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コントロール プレーン プレーン フレーム ドロップのカウントを表示します。
interface interface-id	(任意) 指定された物理インターフェイスのコントロール プレーン情報を表示します。
rate	(任意) CPU ポリサー用に設定されたしきい値レートを表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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、スイッチの UNI および ENI に適用されるポリサー情報を表示します。レイヤ 2 制御プロトコル (CDP、STP、LLDP、LACP、または PAgP) がイネーブルになっている ENI を除いて、レート制限およびポリサーは両方のポートタイプで同じです。

出力には、CPU 保護がディセーブルになっているかどうかも表示されます。

show policer cpu uni-eni drop 特権 EXEC コマンドでは、スイッチ上の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受け入れられたフレーム数およびドロップされたフレーム数が表示されます。

show policer cpu uni-eni rate コマンドでは、**policer cpu uni rate** 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設定されたスイッチ上の CPU 保護レート制限しきい値、またはデフォルトレートである 16000 ビット/秒 (bps) 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。

■ show policer cpu uni-eni

例

次の例では、**show policer cpu uni-eni drop** コマンドの出力を示します。

```
Switch# show policer cpu uni-eni drop
=====
Port          In          Dropped
Name          Frames     Frames
Fa0/1         300        0
Fa0/2         0          0
Fa0/3         0          0
Fa0/4         0          0
Fa0/5         200        0
Fa0/6         0          0
Fa0/7         0          0
Fa0/8         0          0
Fa0/9         508055    325086
Fa0/10        0          0
Fa0/11        0          0
Fa0/12        0          0
Fa0/13        0          0
Fa0/14        0          0
Fa0/15        0          0
Fa0/16        0          0
Fa0/17        0          0
Fa0/18        0          0
Fa0/19        0          0
Fa0/20        0          0
Fa0/21        0          0
Fa0/22        0          0
Fa0/23        0          0
Fa0/24        0          0
Gi0/1         0          0
Gi0/2         0          0
drop-all     0          1849645
```

次の例では、**show policer cpu uni-eni drop interface** コマンドの新しい出力形式を示します。

```
Switch# show policer cpu uni-eni drop interface gigabitethernet 0/1
=====
Policer assigned for Gi0/2
=====
Protocols using this policer:
"VTP" "CISCO_L2" "KEEPALIVE" "SWITCH_IGMP" "SWITCH_L2PT"
Policer rate: 160000 bps
In frames: 48014
Drop frames: 28630
```

次の例では、デフォルト レートが使用されている場合の **show policer cpu uni-eni rate** コマンドの出力を示します。

```
Switch> show policer cpu uni-eni rate
CPU UNI/ENI port police rate = 160000 bps
```

次に、CPU 保護がディセーブルになっているときの show コマンドの出力例を示します。

```
Switch# show policer cpu uni-eni rate
CPU Protection feature is not enabled
```

関連コマンド

コマンド	説明
policer cpu uni	スイッチの CPU ポリサーしきい値レートを設定するか、CPU 保護をイネーブルまたはディセーブルにします。
show platform policer cpu	すべてのポートまたは指定されたポートの割り当て済みポリサー インデックスおよび対応する機能を表示します。

show policy-map

着信および発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、および分類されたトラフィックに対して実行されるアクションを表示するには、**show policy-map** ユーザ EXEC コマンドを使用します。

```
show policy-map [policy-map-name] interface [interface-id] [input | output] [class
class-name]] {begin | exclude | include} expression]
```

構文の説明

<i>policy-map-name</i>	(任意) 指定されたポリシー マップの名前を表示します。
class <i>class-map-name</i>	(任意) 各クラスの QoS ポリシー アクションを表示します。
interface [<i>interface-id</i>] [input output]	(任意) すべてのポートまたは指定したポートに適用したポリシー マップについての情報および統計情報を表示します。ポートを指定する場合、追加のキーワードを指定できます。キーワードには次の意味があります。 <ul style="list-style-type: none"> interface-id : 指定された物理インターフェイスのポリシー マップに関する情報を表示します。 input : スイッチの入力ポリシー マップ、または指定されたポートに適用された入力ポリシー マップについての情報を表示します。 output : スイッチの出力ポリシー マップ、または指定されたポートに適用された出力ポリシー マップについての情報を表示します。
class <i>class-name</i>	(任意) 各クラスのポリシーマップ統計情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 interface** コマンドの出力を示します。

```
Switch> show policy-map interface
GigabitEthernet0/1

Service-policy input: L3

Class-map: dscp-44 (match-all)
  0 packets
  Match: ip dscp 44
```

```
police cir 68000000 bc 1000000
  conform-action set-dscp-transmit af41
  conform-action set-cos-transmit 3
  conform-action set-qos-transmit 18
  exceed-action set-dscp-transmit cs5
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps

Class-map: dscp-14 (match-any)
  0 packets
  Match: ip dscp af13 (14)
  police cir 3000000 bc 93750 pir 5000000 be 156250
    conform-action set-prec-transmit 2
    conform-action set-cos-transmit precedence
    conform-action set-qos-transmit 12
    exceed-action set-cos-transmit precedence table tm-prec-to-cos
    exceed-action set-prec-transmit precedence
    violate-action set-cos-transmit 0
    violate-action set-dscp-transmit af13
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
violate: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps, violate: 0 bps

Class-map: prec-5 (match-any)
  0 packets
  Match: ip precedence 5
  police cir 15000000 bc 468750 pir 16000000 be 500000
    conform-action transmit
    exceed-action set-dscp-transmit precedence
    violate-action set-cos-transmit dscp
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
violate: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps, violate: 0 bps

Class-map: dscp-2 (match-all)
  0 packets
  Match: ip dscp 2
  police cir 34000000 bc 1000000 pir 37000000 be 1000000
    conform-action transmit
    exceed-action drop
    violate-action set-dscp-transmit af41
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
violate: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps, violate: 0 bps

Class-map: prec-0 (match-any)
  0 packets
  Match: ip precedence 0
  police aggregate AP-L3-42m-2
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
violate: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps, violate: 0 bps
NOTE: Policing statistics for a class configured with an aggregate policer are the
same for all classes in the policy-map configured with the same aggregate policer

<output truncated>
```

次の例では、特定のポリシー マップに対する **show policy-map** コマンドの出力を示します。

```
Switch> show policy-map top2
Policy Map top2
  Class class-default
    shape average 11111124
    service-policy pout
```

次の例では、出力ポリシー マップに対する **show policy-map** コマンドの出力を示します。

```
Switch> show policy-map pout
Policy Map pout
  Class ip1
    priority
    police cir percent 10
      conform-action transmit
      exceed-action drop
    queue-limit 250
    queue-limit precedence 1 100
  Class ip2
    Average Rate Traffic Shaping
    cir 5%
  Class ip3
    bandwidth percent 10
    queue-limit 200
    queue-limit precedence 3 100
```

次の例では、入力ポリシー マップに対する **show policy-map** コマンドの出力を示します。

```
Switch> show policy-map pin-police
Policy Map pin-police
  Class ip1
    police cir 20000000 bc 625000
      conform-action transmit
      exceed-action drop
      violate-action drop
```

次の例では、2 レベルの出力ポリシー マップが適用されたインターフェイスに対する **show policy-map interface** コマンドの出力を示します。

```
Switch> show policy-map interface fastethernet0/3
FastEthernet0/3

Service-policy output: top2

Class-map: class-default (match-any)
  209871 packets
  Match: any
    56 packets
  Traffic Shaping
    Average Rate Traffic Shaping
    CIR 11111124 (bps)
  Output Queue:
    Tail Packets Drop: 195421

Service-policy : pout

Class-map: ip1 (match-all)
  9309 packets
  Match: ip precedence 1
  Priority
  police cir 20000000 bc 625000
    conform-action transmit
    exceed-action drop
  conform: 4916 (packets) exceed: 4393 (packets)
```

```

Queue Limit
  queue-limit 250 (packets)
  queue-limit precedence 1 100 (packets)
Output Queue:
  Max Tail Drop Threshold: 250
  Tail Packets Drop: 4393

Class-map: ip2 (match-all)
  0 packets
  Match: ip precedence 2
  Traffic Shaping
    Average Rate Traffic Shaping
    CIR 5%      555555 (bps)
  Output Queue:
    Max Tail Drop Threshold: 48
    Tail Packets Drop: 0

Class-map: ip3 (match-all)
  0 packets
  Match: ip precedence 3
  Bandwidth percent 10      1111110 (bps)
  Queue Limit
    queue-limit 200 (packets)
    queue-limit precedence 3 100 (packets)
  Output Queue:
    Max Tail Drop Threshold: 200
    Tail Packets Drop: 0

Class-map: class-default (match-any)
  200562 packets
  Match: any
    56 packets
  Output Queue:
    Tail Packets Drop: 191028

```

表 2-20 に、**show policy-map interface** の表示のフィールドを示します。表のフィールドは、関連する QoS 機能に従ってグループ化されています。

表 2-20 **show policy-map interface** のフィールドの説明

フィールド	説明
クラスまたはサービス ポリシーに関連付けられたフィールド	
Service-policy input/output	指定されたインターフェイスに適用されている入力または出力サービス ポリシーの名前。
Class-map	表示されているトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択 (match-all または match-any) もトラフィック クラスの横に表示される場合があります。
packets	トラフィック クラスに属すると確認されたパケット数。
Match	トラフィックのクラスに指定された一致基準。これには、サービス クラス (CoS) 値、IP precedence 値、DiffServ コード ポイント (DSCP) 値、アクセス グループ、QoS グループなどの基準が含まれます。
ポリシングに関連付けられたフィールド	
police	トラフィック ポリシングをイネーブルにするために police コマンドが設定されている場合に表示されます。パケットのポリシングに使用される、指定された認定情報レート (CIR) および適合バースト サイズ (BC) が表示されます。

表 2-20 show policy-map interface のフィールドの説明 (続き)

フィールド	説明
conform-action	指定したレートに適合するとしてマーキングされたパケットに対して実行されるアクションを表示します。
conform	指定したレートに適合するとしてマーキングされたパケット数を表示します。
exceed-action	指定したレートを超過するとしてマーキングされたパケットに対して実行されるアクションを表示します。
exceed	指定したレートを超過するとしてマーキングされたパケット数を表示します。
violate-action	最大レートを超過するとしてマーキングされたパケットに対して実行されるアクションを表示します。
violate	最大レートを超過するとしてマーキングされたパケット数を表示します。
キューイングに関連付けられたフィールド	
Queue Limit	クラスに対して設定されたキュー サイズ (パケット数)。
Output Queue	このトラフィック クラス用に作成されるキュー。
Tail packets dropped	キューの深さの平均が最大しきい値を上回る場合にドロップされたパケット数。
トラフィックのスケジューリングに関連付けられたフィールド	
Traffic shaping	シェーピング トラフィックに使用されるレート。
Bandwidth	このクラスに設定された帯域幅 (kb/秒またはパーセンテージ)。
Priority	このクラスにプライオリティ キューイングが設定されていることを示します。

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 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	(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は物理ポート (タイプ、モジュール、ポート番号など) を含みます。
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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。

show port-security

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)
-----
      Gi0/1          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 gigabitethernet0/1
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
        -----
        -----
        -----
1       0006.0700.0800  SecureConfigured   Gi0/2    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 gigabitethernet0/2 address** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet0/2 address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
        -----
        -----
        -----
1       0006.0700.0800  SecureConfigured   Gi0/2    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 gigabitethernet0/2 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 port-type

Cisco CGS 2520 スイッチのインターフェイス タイプの情報を表示するには **show port-type** 特権 EXEC コマンドを使用します。

```
show port-type [eni | nni | uni] [ | {begin | exclude | include} expression]
```

構文の説明

eni	拡張ネットワーク インターフェイスです。
nni	ネットワーク ノード インターフェイスです。
uni	ユーザ ネットワーク インターフェイスです。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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でこのコマンドを入力すると、スイッチのすべてのポートのインターフェイス タイプの情報が出力されます。ポート タイプ (**eni**、**nni**、**uni**) を指定すると、指定したポート タイプの情報が出力されます。

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 port-type** コマンドの出力を示します。

```
Switch# show port-type
Port      Name      Vlan      Port Type
-----
Fa0/1     Fa0/1     1         User Network Interface (uni)
Fa0/2     Fa0/2     1         User Network Interface (uni)
Fa0/3     Fa0/3     1         User Network Interface (uni)
Fa0/4     Fa0/4     1         User Network Interface (uni)
Fa0/5     Fa0/5     1         User Network Interface (uni)
Fa0/6     Fa0/6     1         User Network Interface (uni)
Fa0/7     Fa0/7     1         User Network Interface (uni)
Fa0/8     Fa0/8     1         User Network Interface (uni)
Fa0/9     Fa0/9     1         User Network Interface (uni)
Fa0/10    Fa0/10    1         User Network Interface (uni)
Fa0/11    Fa0/11    1         User Network Interface (uni)
Fa0/12    Fa0/12    1         User Network Interface (uni)
Fa0/13    Fa0/13    1         User Network Interface (uni)
Fa0/14    Fa0/14    1         User Network Interface (uni)
Fa0/15    Fa0/15    1         User Network Interface (uni)
Fa0/16    Fa0/16    1         User Network Interface (uni)
```

```

Fa0/17          routed    User Network Interface (uni)
Fa0/18          1        User Network Interface (uni)
Fa0/19          1        User Network Interface (uni)
Fa0/20          1        User Network Interface (uni)
Fa0/21          1        User Network Interface (uni)
Fa0/22          1        User Network Interface (uni)
Fa0/23          10       User Network Interface (uni)
Fa0/24          10       User Network Interface (uni)
Gi0/1           1        Network Node Interface (nni)
Gi0/2           1        Network Node Interface (nni)

```

次の例では、キーワードを指定した場合の **show port-type** コマンドの出力を示します。

```

Switch# show port-type nni | exclude GigabitEthernet0/1
Port      Name          Vlan      Port Type
-----
Gi0/2          1          Network Node Interface (nni)

```

関連コマンド

コマンド	説明
port-type	特定のポートのインターフェイス タイプを変更します。

show power inline

指定した Power over Ethernet (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 [police] [interface-id | consumption] [ | {begin | exclude | include}
expression]
```

構文の説明

police	(任意) リアルタイムの電力消費に関するパワー ポリシング情報を表示します。
<i>interface-id</i>	(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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 power inline** コマンドの出力を示します。表 2-21 に、出力フィールドの説明を示します。

```
Switch> show power inline
Available:170.0 (w)   Used:76.8 (w)   Remaining:93.2 (w)

Interface Admin  Oper      Power   Device          Class Max
-----
Fa0/17    auto    on        15.4    Cisco PD        n/a  15.4
Fa0/18    auto    on        10.3    IP Phone 7970   3    15.4
Fa0/19    auto    on        12.0    IP Phone 7975   3    15.4
Fa0/20    auto    on        12.0    IP Phone 7975   3    15.4
Fa0/21    auto    on        14.9    Ieee PD         3    20.0
Fa0/22    auto    off       0.0    n/a             n/a  15.4
Fa0/23    auto    on        12.2    AIR-LAP1131AG-A-K9  3    15.4
Fa0/24    auto    off       0.0    n/a             n/a  15.4
```

次の例では、スイッチポートに対する **show power inline police interface-id** コマンドの出力を示します。表 2-21 に、出力フィールドの説明を示します。

```
Switch> show power inline fastethernet0/24
Interface Admin Oper      Power  Device          Class Max
-----
Fa0/24    auto  off      0.0    n/a             n/a  15.4

Interface  AdminPowerMax  AdminConsumption
(Watts)      (Watts)
-----
Fa0/24          15.4          15.4
```

表 2-21 show power inline のフィールドの説明

フィールド	説明
Available	PoE スイッチでの設定電力 ¹ の合計で、ワット数 (W) です。
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計 (ワット数) です。 (Available - Used = Remaining)
Admin	管理モード : auto、off、static
Oper	動作モード : <ul style="list-style-type: none"> 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過しています。
Power	受電装置に割り当てられている最大電力の合計で、ワット数です。この値は、 show power inline police コマンドの出力の <i>Cutoff Power</i> フィールドの値と同じです。
Device	検出された装置のタイプ : n/a、unknown、Cisco 受電装置、IEEE 受電装置、または CDP からの名前。
Class	IEEE 分類 : n/a または 0 ~ 4 の値。
Max	受電装置に割り当てられている最大電力の合計で、ワット数です。
AdminPowerMax	スイッチがリアルタイム電力消費をポリシングする場合に、受電装置に割り当てられる電力の最大量です (ワット単位)。この値は、 <i>Max</i> フィールドの値と同じです。
AdminConsumption	スイッチがリアルタイム電力消費をポリシングする場合に、受電装置に割り当てられる電力の消費量です (ワット単位)。ポリシングがディセーブルである場合、この値は <i>AdminPowerMax</i> フィールドの値と同じです。

1. 設定電力とは、手動で指定する電力、または CDP パワー ネゴシエーションまたは IEEE 分類を使用してスイッチが指定する電力 (パワー センシング機能によってモニタされるリアルタイムの電力とは異なります) です。

show power inline

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
Interface  Consumption      Admin
           Configured  Consumption (Watts)
-----
Fa0/17     NO                0.0
Fa0/18     YES               10.3
Fa0/19     YES               12.0
Fa0/20     NO                0.0
Fa0/21     NO                0.0
Fa0/22     NO                0.0
Fa0/23     NO                0.0
Fa0/24     NO                0.0
```

次の例では、**show power inline police** コマンドの出力を示します。表 2-22 に、出力フィールドの説明を示します。

```
Switch> show power inline police
Available:170.0(w)  Used:76.8(w)  Remaining:93.2(w)

Interface Admin  Oper      Admin      Oper      Cutoff Oper
          State State      Police      Police      Power  Power
-----
Fa0/17   auto  on        none       n/a       n/a    4.6
Fa0/18   auto  on        log        ok        12.0   6.5
Fa0/19   auto  on        errdisable ok        12.0   5.1
Fa0/20   off   off       none       n/a       n/a    0.0
Fa0/21   auto  on        log        log        6.0    7.6
Fa0/22   auto  off       none       n/a       n/a    0.0
Fa0/23   auto  errdisable errdisable n/a       12.0   0.0
Fa0/24   off   off       errdisable n/a       12.0   0.0
-----
Totals:                                23.8
```

上の例では、次のようになっています。

- Fa0/17 ポートは起動していて、受電装置に接続され、ポリシングはディセーブルになっています。
- Fa0/18 ポートは起動していて、受電装置に接続され、ポリシングがイネーブルになっています。ポリシングアクションによって Syslog メッセージが生成されます。リアルタイム電力消費がカットオフ値より少ないため、ポリシングアクションは作動しません。
- Fa0/19 ポートは起動していて、受電装置に接続され、ポリシングがイネーブルになっています。ポリシングアクションによってポートはシャットダウンされます。リアルタイム電力消費がカットオフ値より少ないため、ポリシングアクションは作動しません。
- Fa0/20 ポートでは、装置検出がディセーブルで、ポートに電力は適用されず、ポリシングがディセーブルになっています。
- Fa0/21 ポートは起動していて、受電装置に接続され、ポリシングがイネーブルになっています。ポリシングアクションによって Syslog メッセージが生成されます。
- Fa0/22 ポートは起動していてポリシングはディセーブルですが、スイッチは接続装置に電力を供給しません。
- Fa0/23 ポートは起動していて、受電装置に接続され、ポリシングがイネーブルになっています。ポリシングアクションによってポートはシャットダウンされます。
- Fa0/24 ポートでは、装置検出がディセーブルで、電力はポートに適用されませんが、ポリシングがイネーブルになっています。ポリシングアクションによってポートがシャットダウンされます。

次の例では、スタンドアロン スイッチに対する **show power inline police interface-id** コマンドの出力を示します。表 2-22 に、出力フィールドの説明を示します。

```
Switch> show power inline police fastethernetfa0/20
Interface Admin Oper      Admin      Oper      Cutoff Oper
           State State      Police     Police     Power   Power
-----
Fa0/20    auto   on        errdisable ok         12.0    4.7
```

表 2-22 show power inline police のフィールドの説明

フィールド	説明
Available	スイッチでの設定電力 ¹ の合計で、ワット数 (W) です。
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計 (ワット数) です。 (Available - Used = Remaining)
Admin State	管理モード : auto、off、static
Oper State	動作モード : <ul style="list-style-type: none"> errdisable : ポリシングはイネーブルです。 faulty : 受電装置での装置検出が障害の状態です。 off : PoE が適用されていません。 on : 受電装置が検出され、電力が適用されています。 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、リアルタイム電力消費が最大電力割り当てを超えています。 <p>(注) 動作モードは、指定した PoE ポートまたはスイッチのすべての PoE ポートの現在の PoE ステータスです。</p>
Admin Police	リアルタイム電力消費ポリシング機能のステータス : <ul style="list-style-type: none"> errdisable : ポリシングがイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチはポートをシャットダウンします。 log : ポリシングはイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチが Syslog メッセージを生成します。 none : ポリシングはディセーブルです。
Oper Police	ポリシング ステータス : <ul style="list-style-type: none"> errdisable : リアルタイム電力消費が最大電力割り当てを超えています。スイッチが PoE ポートをシャットダウンします。 log : リアルタイム電力消費が最大電力割り当てを超えています。スイッチが Syslog メッセージを生成します。 n/a : 装置検出がディセーブルで、電力が PoE ポートに適用されていないか、ポリシングアクションが設定されていません。 ok : リアルタイム電力消費が最大電力割り当てより少ない状態です。
Cutoff Power	ポートに割り当てられている最大電力です。リアルタイム電力消費がこの値を上回ると、スイッチは設定されたポリシングアクションを実行します。
Oper Power	受電装置のリアルタイム電力消費です。

1. 設定電力とは、手動で指定する電力、または CDP パワー ネゴシエーションまたは IEEE 分類を使用してスイッチが指定する電力 (パワー センシング機能によってモニタされるリアルタイムの電力とは異なります) です。

■ show power inline

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 rep topology

セグメント内のプライマリ エッジ ポートおよびセカンダリ エッジ ポートを含む特定のセグメントまたはすべてのセグメントについて Resilient Ethernet Protocol (REP) トポロジ情報を表示するには、**show rep topology** ユーザ EXEC コマンドを使用します。

```
show rep topology [segment segment_id] [archive] [detail] [| {begin | exclude | include}
expression]
```

構文の説明

segment-id	(任意) 指定されたセグメントの REP トポロジ情報を表示します。指定できる ID 範囲は 1 ~ 1024 です。
archive	(任意) セグメントの前のトポロジを表示します。このキーワードは、リンク障害のトラブルシューティングに役立ちます。
detail	(任意) REP トポロジの詳細情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。6/16

使用上のガイドライン

show rep topology コマンドの出力では、エッジ、ネイバーなしに設定されているポートは *Pri* または *Sec* の前にアスタリスク (*) で示されます。**show rep topology detail** コマンドの出力では、*No-Neighbor* と表示されます。

このコマンドの出力は **show tech-support** 特権 EXEC コマンドの出力にも含まれています。

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

次の例は、**show rep topology segment** 特権 EXEC コマンドの出力を示します。

```
Switch # show rep topology segment 1
REP Segment 1
BridgeName      PortName      Edge Role
-----
sw1_multseg_3750 Gi1/1/1      Pri  Alt
sw3_multseg_2520 Gi0/13              Open
sw3_multseg_2520 Gi0/14              Alt
sw4_multseg_2520 Gi0/13              Open
sw4_multseg_2520 Gi0/14              Open
sw5_multseg_2520 Gi0/13              Open
sw5_multseg_2520 Gi0/14              Open
sw2_multseg_3750 Gi1/1/2              Open
```

■ show rep topology

```
sw2_multseg_3750 Gi1/1/1      Open
sw1_multseg_3750 Gi1/1/2      Sec Open
```

次の例では、エッジポートに REP ネイバーがない構成の場合の **show rep topology** コマンドの出力を示します。

```
Switch # show rep topology
REP Segment 2
BridgeName      PortName      Edge  Role
-----
sw8-ts8-51      Gi0/2         Pri*  Open
sw9-ts11-50     Gi1/0/4              Open
sw9-ts11-50     Gi1/0/2              Open
sw1-ts11-45     Gi0/2          Alt
sw1-ts11-45     Po1            Open
sw8-ts8-51      Gi0/1         Sec*  Open
```

次の例は、**show rep topology detail** コマンドの出力を示します。

```
Switch# show rep topology detail
REP Segment 2
repc_2_24ts, Fa0/2 (Primary Edge)
  Alternate Port, some vlans blocked
  Bridge MAC: 0019.e714.5380
  Port Number: 004
  Port Priority: 080
  Neighbor Number: 1 / [-10]
repc_3_12cs, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 001
  Port Priority: 000
  Neighbor Number: 2 / [-9]
repc_3_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 3 / [-8]
repc_4_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a19d.7c80
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 4 / [-7]
repc_4_12cs, Gi0/2 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 001a.a19d.7c80
  Port Number: 002
  Port Priority: 040
  Neighbor Number: 5 / [-6]
```

<output truncated>

次の例は、**show rep topology segment archive** コマンドの出力を示します。

```
Switch# show rep topology segment 1 archive
REP Segment 1
BridgeName      PortName      Edge Role
-----
sw1_multseg_3750 Gi1/1/1      Pri  Open
sw3_multseg_2520 Gi0/13              Open
sw3_multseg_2520 Gi0/14              Open
sw4_multseg_2520 Gi0/13              Open
sw4_multseg_2520 Gi0/14              Open
sw5_multseg_2520 Gi0/13              Open
sw5_multseg_2520 Gi0/14              Open
sw2_multseg_3750 Gi1/1/2              Alt
sw2_multseg_3750 Gi1/1/1              Open
sw1_multseg_3750 Gi1/1/2      Sec  Open
```

関連コマンド

コマンド	説明
rep segment	インターフェイス上で REP をイネーブルにし、セグメント ID を割り当てます。このコマンドは、ポートをエッジポート、プライマリエッジポート、または優先ポートとして設定するためにも使用されます。

show scada modbus tcp server

MODBUS TCP サーバ情報を表示するには、**show scada modbus tcp server** 特権 EXEC コマンドを使用します。

```
show scada modbus tcp server [connections] [ | {begin | exclude | include} expression]
```

構文の説明

connections	(任意) クライアント情報と統計情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	(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

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

サーバ情報および統計情報のみを表示するには、**show scada modbus tcp server** コマンドを使用します。クライアント情報および統計情報のみを表示するには、**connections** キーワードを使用します。

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

次の例は、**show scada modbus tcp server** コマンドの出力を示します。

```
Switch# show scada modbus tcp server
Summary: enabled, running, process id 142

Conn Stats: listening on port 801, 4 max simultaneous connections
             0 current client connections
             0 total accepted connections, 0 accept connection errors
             0 closed connections, 0 close connection errors

Send Stats: 0 tcp msgs sent, 0 tcp bytes sent, 0 tcp errors
            0 responses sent, 0 exceptions sent, 0 send errors

Recv Stats: 0 tcp msgs received, 0 tcp bytes received, 0 tcp errors
            0 requests received, 0 receive errors
```

関連コマンド

コマンド	説明
clear scada modbus tcp server statistics	MODBUS TCP サーバおよびクライアントの統計情報をクリアします。
scada modbus tcp server	スイッチ上で MODBUS TCP をイネーブルにします。スイッチは、MODBUS TCP サーバとして機能します。

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 [default | dual-ipv4-and-ipv6 {default | routing | vlan} | layer-2] [|
  {begin | exclude | include} expression]
```



(注) **default** および **dual-ipv4-and-ipv6** キーワードは、スイッチ上にメトロ IP アクセス イメージがインストールされている場合にのみ表示されます。

構文の説明

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。 <ul style="list-style-type: none"> • 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。
layer-2	(任意) レイヤ 2 機能をサポートし、ルーティングをサポートしないテンプレートのリソース割り当てを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマン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。

表示される番号は、各機能のリソースのおおよその最大数を表します。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。

show sdm prefer

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 'layer-2' 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:          8K
number of IPv4 IGMP groups:              1K
number of IPv4 multicast routes:         0
number of unicast IPv4 routes:          0
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:            512
number of IPv4/MAC security aces:       1K
```

次に、**show sdm prefer default** コマンドの出力例を示します。

```
Switch# show sdm prefer default
"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:          5K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:          9K
  number of directly-connected IPv4 hosts: 5K
  number of indirect IPv4 routes:       4K
number of IPv4 policy based routing aces: 512
number of IPv4/MAC qos aces:            512
number of IPv4/MAC security aces:       1K
```

次に、**show sdm prefer dual-ipv4-and-ipv6 routing** コマンドの出力例を示します。

```
Switch# show sdm prefer dual-ipv4-and-ipv6 routing
"desktop IPv4 and IPv6 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:          1.5K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:          2.75K
  number of directly-connected IPv4 hosts: 1.5K
  number of indirect IPv4 routes:       1.25K
number of IPv6 multicast groups:         1.125k
number of directly-connected IPv6 addresses: 1.5K
number of indirect IPv6 unicast routes:  1.25K
number of IPv4 policy based routing aces: 0.25K
number of IPv4/MAC qos aces:            0.75K
number of IPv4/MAC security aces:       0.5K
number of IPv6 policy based routing aces: 0.25K
number of IPv6 qos aces:                0.5K
number of IPv6 security aces:          0.5K
```

関連コマンド

コマンド	説明
sdm prefer	レイヤ 2 機能に対してリソースを最大化するように SDM テンプレートを設定するか、または SDM テンプレートをデフォルト テンプレートに設定します。

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] | blockedports | bridge | detail [active]
| inconsistentports | interface interface-id | mst | pathcost method | root | summary
[totals] | 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

<i>bridge-group</i>	(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)。
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 <i>interface-id</i> [active [detail] cost detail [active] inconsistency portfast priority rootcost state]	<p>(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、物理ネットワーク ノード インターフェイス (NNI)、拡張ネットワーク インターフェイス (ENI)、VLAN、および NNI または ENI ポート チャンネルが含まれます。指定できる VLAN 範囲は 1 ~ 4094 です。ポート チャンネル範囲は 1 ~ 48 です。</p> <p>(注) スパニング ツリー プロトコル (STP) は、ユーザ ノード インターフェイス (UNI) ではサポートされていません。UNI インターフェイス ID を入力した場合、スパニング ツリー情報は表示されません。</p>
mst [configuration [digest]] [instance-id [detail interface interface-id [detail]]]	<p>(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)。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • 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)。 <p>IEEE 標準の実装のために専門用語が更新され、<i>txholdcount</i> フィールドが追加されました。</p> <p>境界ポート用に新しいマスター ロールが表示されます。</p> <p>IEEE 標準ブリッジがポートに先行標準 BPDU を送信した場合、<i>pre-standard</i> または <i>Pre-STD</i> という用語が表示されます。</p> <p>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、<i>pre-standard (config)</i> または <i>Pre-STD-Cf</i> という用語が表示されます。</p> <p>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、<i>pre-standard (rcvd)</i> または <i>Pre-STD-Rx</i> という用語が表示されます。</p> <p>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、<i>dispute</i> フラグが表示されます。</p> <ul style="list-style-type: none"> • 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、VLAN、物理 NNI と NNI ポート チャンネル、および物理 ENI と ENI ポート チャンネルが含まれます。UNI では STP はサポートされていません。指定できる VLAN 範囲は 1 ~ 4094 です。ポート チャンネル範囲は 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	<p>(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)。</p>

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。
vlan <i>vlan-id</i> [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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

UNI では STP はサポートされていません。有効なスパニングツリー情報は NNI または ENI でだけ使用できます。

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 (GigabitEthernet0/1)
             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
```

show spanning-tree

```

Interface          Role Sts Cost      Prio.Nbr Type
-----
Gi0/1              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 24 (GigabitEthernet0/1), 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 (GigabitEthernet0/1) 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 gigabitethernet0/1
Vlan              Role Sts Cost      Prio.Nbr Type
-----
VLAN0001          Root FWD 3019     128.24  P2p

```

次の例では、**show spanning-tree summary** コマンドの出力を示します。

```

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
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.

```

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 configuration digest** コマンドの出力を示します。

```
Switch# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision  0      Instances configured 1
Digest    0xAC36177F50283CD4B83821D8AB26DE62
Pre-std Digest 0xBB3B6C15EF8D089BB55ED10D24DF44DE
```

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 gigabitethernet0/1
GigabitEthernet0/1 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 Gi0/1 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
-----
GigabitEthernet0/1 root FWD 200000 128 P2P bound(STP)
GigabitEthernet0/2 desg FWD 200000 128 P2P bound(STP)
Port-channell 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 bpdupfilter	インターフェイスでの Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータ ユニット) 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。
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 を廃棄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 カウントを設定します。
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 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 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

<i>interface-id</i>	(任意) 物理ポートのインターフェイス ID (タイプ、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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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
-----
Gi0/1     Forwarding    20 pps     10 pps     5 pps
Gi0/2     Forwarding    50.00%    40.00%    0.00%
<output truncated>
```

show storm-control

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いないため、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 0/1
Interface      Filter State  Upper      Lower      Current
-----
Gi0/1          Forwarding    20 pps     10 pps     5 pps
```

表 2-23 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 2-23 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。 <ul style="list-style-type: none"> 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 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
	12.2(53)EX	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。ルーティング MTU は、ルーティングされるパケット用の MTU 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 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 1500 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 ポートまたはギガビット イーサネット ポートの MTU サイズを設定します。

show table-map

設定済みのすべてのテーブル マップ、または選択したテーブル マップについての Quality of Service (QoS) テーブルマップ情報を表示するには **show table-map** ユーザ EXEC コマンドを使用します。

```
show table-map [table-map-name] [ | {begin | exclude | include} expression]
```

構文の説明

<i>table-map-name</i>	(任意) テーブル マップの名前。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 table-map** コマンドの出力を示します。

```
Switch> show table-map
tandoori_1>show table-map
Table Map abc
  default copy

Table Map cos2dscp
  from 2 to 16
  default copy

Table Map cos2cos
  from 2 to 5
  from 3 to 6
  default 7

Table Map cos2cos10
  default copy

Table Map cos=cos
  default copy
```

次の例では、特定のテーブル マップ名に対する **show table-map** コマンドの出力を示します。

```
Switch> show table-map tm
```

```
Table Map tm
  from 1 to 62
  from 2 to 63
  default ignore
```

関連コマンド

コマンド	説明
table-map	CoS/DSCP などの、Quality Of Service (QoS) マッピング テーブルを作成します。

show udld

すべてのポートまたは指定されたポートの単一方向リンク検出 (UDLD) 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

<i>interface-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 2-24 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 gigabitethernet0/1
Interface gi0/1
---
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: Gi0/1
  Neighbor echo 1 device: Switch-B
  Neighbor echo 1 port: Gi0/2
  Message interval: 5
```

CDP Device name: Switch-A

表 2-24 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 が実際に稼働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 がネイバー 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	ネイバー 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 デバイスおよびネイバー デバイスの両方で UDLD が通常どおり稼働している場合、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	デバイス名またはネイバーのシステム シリアル番号。デバイス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ネイバー デバイス名。
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。デバイス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** コマンドをユーザ EXEC モードまたは特権 EXEC モードで使します。

show version [| {**begin** | **exclude** | **include**} *expression*]

構文の説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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 およびユーザ EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	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 IOS Software, CGS2520 Software (CGS2520-IPSERVICESK9-M), Experimental Version 12.2
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 16-Apr-10 14:56 by jdoe
Image text-base: 0x01000000, data-base: 0x02F00000
```

```
ROM: Bootstrap program is CGS2520 boot loader
BOOTLDR: CGS2520 Boot Loader (CGS2520-HBOOT-M), Version 12.2
```

```
switch uptime is 11 minutes
System returned to ROM by power-on
System image file is "flash:cgs2520-ip-servicesk9-mz"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to
export@cisco.com.

```
cisco CGS-2520-16S-8PC (PowerPC405) processor (revision 01) with 262144K bytes of memory.
Processor board ID FOC1411X1LZ
Last reset from power-on
Target IOS Version 12.2(46)SE
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
```

512K bytes of flash-simulated non-volatile configuration memory.

```
Base ethernet MAC Address      : FC:FB:FB:6C:8E:00
Motherboard assembly number    : 73-12492-02
Motherboard serial number      : FOC14094FGD
Model revision number          : 01
Motherboard revision number    : 07
Model number                   : CGS-2520-16S-8PC
System serial number           : FOCABCD1234
Top Assembly Part Number       : 800-32559-01
Top Assembly Revision Number   : 42
Version ID                     : V01
CLEI Code Number               : ABCDEFGHIJ
Hardware Board Revision Number : 0x02
FPGA Version                   : 79
```

Switch	Ports	Model	SW Version	SW Image
*	1 26	CGS-2520-16S-8PC	12.2 (20100417:214633)	CGS2520-IPSERVICESK9-M

Configuration register is 0xF

show vlan

スイッチ上のすべての設定済みの VLAN または特定の 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 [access-map | brief | dot1q tag native | filter | id vlan-id | internal usage | mtu
| name vlan-name | private-vlan [type] | remote-span | summary | uni-vlan [type]]
[ | {begin | exclude | include} expression ]
```

構文の説明

access-map	show vlan access-map コマンドを参照してください。
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。このキーワードは、スイッチでメトロ IP アクセス イメージまたはメトロ アクセス イメージが稼動している場合のみサポートされます。
filter	show vlan filter コマンドを参照してください。
id <i>vlan-id</i>	(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。 <i>vlan-id</i> 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 1006 ~ 4094) からのものです。これらの ID を持つ VLAN は、内部使用のリストから削除しない限り、 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作成できません。このキーワードを使用できるのは、スイッチでメトロ IP アクセス イメージが実行されている場合だけです。
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 <i>vlan-name</i>	(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 [<i>type</i>]	(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。VLAN ID およびプライベート VLAN のタイプだけを参照するには、 type を入力します (任意)。
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。
uni-vlan [<i>type</i>]	(任意) ユーザ ネットワーク インターフェイス-拡張ネットワーク インターフェイス (UNI-ENI) VLAN 情報を表示します。VLAN ID および UNI-ENI VLAN のタイプだけを参照するには、 type を入力します (任意)。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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tring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	変更箇所
12.2(53)EX	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 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* と表示されている場合、異なる MTU を持つ複数のポートが VLAN に存在していることを意味します。大きな MTU のポートから小さな MTU のポートにスイッチングされたパケットは、ドロップされる可能性があります。VLAN にスイッチ仮想インターフェイス (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、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* 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。

show vlan uni-vlan type コマンドの出力では、タイプは *community* または *isolated* です。UNI-ENI コミュニティ VLAN 内のユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) は、相互に通信できます。UNI-ENI 隔離 VLAN 内の UNI または ENI は、相互に通信できません。ネットワーク ノード インターフェイス (NNI) は、相互に通信できます。また、UNI-ENI 隔離およびコミュニティ VLAN 内の UNI または ENI とも通信できます。

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 vlan** コマンドの出力を示します。表 2-25 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)

スイッチは、イーサネット VLAN だけをサポートしています。FDDI およびトークンリング VLAN のパラメータを設定して、vlan.dat ファイルでの結果を表示できますが、これらのパラメータはサポートされていないか、または使用されません。

```
Switch> show vlan
Switch#show vlan
VLAN Name                Status      Ports
-----
1    default                active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gi0/1, Gi0/2

1002 fddi-default          act/unsup
1003 token-ring-default     act/unsup
```

show vlan

```

1004 fddinet-default          act/unsup
1005 trnet-default           act/unsup

VLAN Type SAID      MTU   Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001    1500 -     -     -        -   -         0     0
1002 fddi  101002    1500 -     -     -        -   -         0     0
1003 tr   101003    1500 -     -     -        -   -         0     0
1004 fdnet 101004    1500 -     -     -        ieee -         0     0
1005 trnet 101005    1500 -     -     -        ibm  -         0     0
                                OVLAN Name

Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----

VLAN Type          Ports
-----

```

表 2-25 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 Source-Route Bridging (SRB; ソースルートブリッジング) および Source-Route Transparent (SRT; ソースルートトランスペアレント) で、デフォルトは SRB です。
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。
VLAN Type/Ports	設定されている UNI-ENI VLAN、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表示します。

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 Gi0/3
10 502 community Fa0/11
10 503 non-operational3 -
20 25 isolated Fa0/13, Fa0/20, Fa0/22, Gi0/1,
20 30 community Fa0/13, Fa0/20, Fa0/21, Gi0/1,
20 35 community Fa0/13, Fa0/20, Fa0/23, Fa0/33. Gi0/1,
20 55 non-operational
2000 2500 isolated Fa0/5, Fa0/10, Fa0/15
```

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 uni-vlan type** コマンドの出力を示します。

```
Switch> show vlan uni-vlan type
Vlan Type
-----
1 UNI isolated
20 UNI community
201 UNI isolated
```

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 : 0
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 Gi0/1, Gi0/2

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
2 enet 100002 1500 - - - - - 0 0

Remote SPAN VLAN
-----
Disabled
```

show vlan

次の例では、**show vlan internal usage** コマンドの出力を示します。VLAN 1025 および 1026 が、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 FastEthernet0/23
1026 FastEthernet0/24
```

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 メンバーシップ モードを設定します。
vlan	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	
<i>mapname</i>	(任意) 特定の VLAN アクセス マップ名。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
	12.2(53)EX	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_Fal_0_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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 vlan mapping

トランク ポートの VLAN マッピングについての情報を表示するには、**show vlan mapping** 特権 EXEC コマンドを使用します。

```
show vlan mapping [interface interface-id | usage] [| {begin | exclude | include}
expression]
```

構文の説明

interface interface-id	(任意) 指定したインターフェイスの VLAN マッピング情報を表示します。
usage	(任意) VLAN マッピングで使用されるハードウェア リソースを表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 mapping** コマンドの出力を示します。

```
Switch# show vlan mapping
Interface Fa0/5:
VLANs on wire      Translated VLAN      Operation
-----
default QinQ      1                    selective QinQ
Interface Fa0/2:
VLANs on wire      Translated VLAN      Operation
-----
2                  104                  1-to-1 mapping
```

■ show vlan mapping

次の例では、インターフェイスの **show vlan mapping** コマンドの出力を示します。

```
Switch# show vlan mapping interface fa0/6
Interface fa0/6:
VLAN on wire      Translated VLAN      Operation
1                 11                   1-to-1 mapping
12,16-18         100                  selective QinQ
*                101                  default QinQ
```

次の例では、**show vlan mapping usage** コマンドの出力を示します。

```
Switch# show vlan mapping usage
Ports:Gi0/1-Gi0/2,Fa0/1-Fa0/24
Vlan Mapping resource usage is 1%
```

```
Switch# show vlan mapping usage
Ports:Gi0/1-Gi0/4
Vlan Mapping resource usage is 0%
```

```
Ports:Gi0/5-Gi0/8
Vlan Mapping resource usage is 0%
```

```
Ports:Gi0/9-Gi0/12
Vlan Mapping resource usage is 0%
```

```
Ports:Gi0/13-Gi0/16
Vlan Mapping resource usage is 0%
```

関連コマンド

コマンド	説明
switchport vlan mapping	インターフェイスで VLAN マッピングを設定します。

show vmmps

VLAN Query Protocol (VQP) バージョン、再確認間隔、再試行回数、VLAN メンバーシップ 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、キーワードを指定せずに **show vmmps** ユーザ EXEC コマンドを使用します。**statistics** キーワードを指定すると、クライアント側の統計情報が表示されます。

```
show vmmps [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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 vmmps statistics** コマンドの出力を示します。

```
Switch> show vmmps 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 2-26 に、表示される各フィールドの説明を示します。

表 2-26 show vmmps 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。

show vmmps

表 2-26 show vmmps statistics のフィールドの説明 (続き)

フィールド	説明
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。エイジング 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 VQP 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	リソースの可用性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 vmmps 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。
vmmps 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。
vmmps 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。
vmmps 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。

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。

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	変更箇所
12.2(53)EX	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。ユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) のデフォルト ステートは、シャットダウンです。UNI または ENI を設定する前に、**no shutdown** コマンドを使用して UNI または ENI をイネーブルにする必要があります。ネットワーク ノード インターフェイス (NNI) はデフォルトでイネーブルです。

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 gigabitethernet0/2
Switch(config-if)# shutdown
```

```
Switch(config)# interface gigabitethernet0/2
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

<i>vlan-id</i>	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。デフォルト VLAN として定義された VLAN (1 および 1002 ~ 1005)、および拡張範囲 VLAN (1006 ~) は、シャットダウンできません。
----------------	---

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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

拡張範囲 VLAN (1006 ~ 4094) を含む VLAN 上のローカルトラフィックをシャットダウンするには、**shutdown VLAN** 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、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 (VLAN コンフィギュレーション)	VLAN コンフィギュレーション 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。

snmp mib rep trap-rate

リンク動作ステータスまたはポート ロールが変更された場合に Resilient Ethernet Protocol (REP; レジリエントイーサネットプロトコル) SNMP トラップを送信するように設定するには、**snmp mib rep trap-rate** 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。REP トラップの送信をディセーブルにするには、コマンドの **no** バージョンを使用します。

snmp mib rep trap-rate value

no snmp mib rep trap-rate

構文の説明

trap-rate value 1 秒間に送信する REP トラップ数を設定します。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 (制限なし、発生するたびにトラップが送信される) です。

デフォルト

REP トラップの送信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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

リンク動作ステータスの変更またはポート ロールの変更に対応する REP 固有のトラップを送信するようにスイッチをイネーブルにするには、このコマンドを使用します。

例

1 秒あたり 10 の割合で REP トラップを送信するようにスイッチを設定する例を示します。

```
Switch(config)# snmp mib rep trap-rate 10
```

関連コマンド

コマンド	説明
show running config	REP トラップが設定されていることを確認します。

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] | 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] |
ethernet | flash | 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] | storm-control trap-rate value | stpx
[inconsistency] [root-inconsistency] [loop-inconsistency] | syslog | transceiver all |
tty | vlan-membership | vlancreate | vlandelete]
```

```
no snmp-server enable traps [bgp | bridge [newroot] [topologychange] | 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] |
ethernet | flash | 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] | storm-control trap-rate value | stpx
[inconsistency] [root-inconsistency] [loop-inconsistency] | syslog | transceiver all |
tty | vlan-membership | vlancreate | vlandelete]
```

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、メトロ IP アクセス イメージがスイッチ上で動作している場合にだけサポートされます。
bridge [newroot] [topologychange]	(任意) スパニング ツリー プロトコル (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。 <ul style="list-style-type: none"> 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。
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]	<p>(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。</p> <ul style="list-style-type: none"> • 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。 <p>(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。</p>
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]	<p>(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。</p> <ul style="list-style-type: none"> • 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。
ethernet	(任意) SNMP イーサネット トラップをイネーブルにします。
flash	(任意) SNMP FLASH 通知をイネーブルにします。
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]	<p>(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。</p> <ul style="list-style-type: none"> • 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]	<p>(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。</p> <ul style="list-style-type: none"> • 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]	<p>(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 (制限なし、ポートセキュリティが発生するたびにトラップが送信される) です。</p>
power-ethernet {group name police}	<p>(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。</p> <ul style="list-style-type: none"> • 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	<p>(任意) SNMP Response Time Reporter トラップをイネーブルにします。</p>
snmp [authentication coldstart linkdown linkup warmstart]	<p>(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。</p> <ul style="list-style-type: none"> • 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。
storm-control trap-rate value	<p>(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。デフォルトは 0 (制限なし、ストーム制御が発生するたびにトラップが送信される) です。</p>

stpx [inconsistency] [root-inconsistency] [loop-inconsistency]	(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。 <ul style="list-style-type: none"> • 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。
transceiver all	(任意) スイッチに取り付けられている、サポートされるすべての Digital Optical Monitoring (DOM) 対応トランシーバについて、SNMP 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 メンバーシップ 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。



(注) **fru-ctrl insertion、removal**、および **vtp** キーワードは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません。**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	変更箇所
12.2(53)EX	このコマン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、すべてのトラップ 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。

snmp-server enable traps

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。

SNMP トランシーバトラップは、スイッチに取り付けられている DoM 対応トランシーバをサポートする SFP に適用されます。センサーの値は 10 分おきにポーリングされ、この頻度でトラップまたはアラームが表示されます。

例

次の例では、NMS にポートセキュリティトラップを送信する方法を示します。

```
Switch(config)# snmp-server enable traps port security
```

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 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
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

<i>host-addr</i>	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 <i>port</i>	(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。 <ul style="list-style-type: none"> 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 <i>vrf-instance</i>	(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。
<i>community-string</i>	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。

(注) **bgp**、**hsrp**、**ipmulticast**、**mdsp**、**ospf**、および **pim** キーワードは、スイッチ上にメトロ IP アクセス イメージがインストールされている場合にのみ使用できます。

- **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、メトロ IP アクセス イメージがスイッチ上にインストールされている場合にだけ有効です。
 - **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。
 - **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。
 - **flash** : SNMP FLASH 通知を送信します。
 - **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。
 - **stp** : 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。
 - **vlan-membership** : SNMP VLAN メンバーシップ 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。
-



(注) **fru-ctrl**、および **vtp** キーワードは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません。

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	変更箇所
12.2(53)EX	このコマン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tring *comaccess* を設定し、この String 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 String 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 String *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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
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	このインターフェイスに MAC アドレスが追加 (added) された場合、MAC アドレス通知トラップをイネーブルにします。
removed	このインターフェイスから MAC アドレスが削除 (removed) された場合、MAC アドレス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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

snmp trap mac-notification 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** および **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 gigabitethernet0/2
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

インターフェイス上でスパニング ツリー インスタンスをイネーブルにするには、拡張ネットワーク インターフェイス (ENI) でキーワードを指定せずに **spanning-tree** 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。デフォルトの設定であるディセーブルに戻すには、このコマンドの **no** 形式を使用します。

spanning-tree

no spanning-tree

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

スパニング ツリー プロトコル (STP) は ENI でディセ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	変更箇所
12.2(53)EX	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、ENI、および ENI を含む EtherChannel ポート チャネルでのみサポートされます。

STP は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされておらず、ENI ではデフォルトでディセーブルになっています。ENI で STP をイネーブルにするには、このコマンドを使用します。ポートを ENI として設定するには、**port-type eni** 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。STP が ENI でイネーブルになると、他のすべての STP インターフェイス コンフィギュレーション コマンドをインターフェイスで使用できるようになります。

スイッチは、1 つの VLAN 上で 1 つのスパニング ツリー インスタンスのみをサポートします。スパニング ツリーがイネーブルになっている NNI および ENI は、同じ VLAN に存在する場合、同じスパニング ツリー インスタンスに属します。

STP は、NNI でデフォルトでイネーブルになっています。UNI は、通常カスタマー側のポートで、サービス プロバイダーのスパニング ツリーには参加しません。ただし、カスタマー側のポートを ENI として設定し、スパニング ツリーをイネーブルにすると、**spanning-tree guard root** 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上のルート ガードを設定しない限り、ENI がスパニング ツリー ルート ポートとなる場合があります。STP がイネーブルに設定されているカスタマー側の ENI は、サービス プロバイダー側の NNI と同じスパニング ツリーに参加します。



(注) カスタマー側の ENI 上の STP をイネーブルにする場合、注意して使用してください。

■ spanning-tree

例 次の例では、ポート上で STP をイネーブルにする方法を示します。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type eni
Switch(config-if)# spanning-tree
```

設定を確認するには、**show spanning-tree 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 spanning-tree interface <i>interface-id</i>	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。

spanning-tree bpdudfilter

インターフェイスがブリッジプロトコルデータユニット (BPDU) を送受信できないようにするには、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) で **spanning-tree bpdudfilter** 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 bpdudfilter {disable | enable}

no spanning-tree bpdudfilter

構文の説明

disable	指定された STP ポート上で 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 STP ポート上で 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパンニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。STP がイネーブルになっている NNI または ENI 上でのみ BPDU フィルタリングを設定できます。ポートを NNI または ENI として設定するには、**port-type {nni | eni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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) モードで稼働している場合は、BPDU フィルタリング機能をイネーブルにできません。



注意

STP ポート上で BPDU フィルタリングをイネーブルにすると、STP ポート上でスパンニング ツリーをディセーブルにしたのと同じ結果になり、スパンニング ツリー ループが発生する可能性があります。

すべての PortFast 対応 STP ポート上で 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 bpdudfilter 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 bpdudfilter インターフェイス コンフィギュレーション コマンドを STP ポートで使用すると、**spanning-tree portfast bpdudfilter 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 gigabitethernet0/1
Switch(config-if)# spanning-tree bpdudfilter 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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
spanning-tree portfast (グローバル コンフィギュレーション)	PortFast 対応 STP ポート上で 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 STP ポートで 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 STP ポート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

ブリッジ プロトコル データ ユニット (BPDU) を受信したインターフェイスを `errdisable` ステートにするには、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張 ネットワーク インターフェイス (ENI) で **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 STP ポートで BPDU ガードをディセーブルにします。
enable	指定された STP ポートで 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパンニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。STP がイネーブルになっている NNI または ENI 上でのみ BPDU ガードを設定できます。ポートを NNI または ENI として設定するには、**port-type {nni | eni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

手動で STP ポートを再び動作させなければならないので、BPDU ガード機能は無効な設定に対する安全対策になります。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ンニング 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) モードで稼働している場合は、BPDU ガード機能をイネーブルにできます。

すべての PortFast 対応 STP ポート上で 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 STP ポートで使用すると、**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 gigabitethernet0/1
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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
spanning-tree portfast (グローバル コンフィギュレーション)	PortFast 対応 STP ポート上で 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 STP ポートで 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 STP ポート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 ツリーの計算に使用するパス コストを設定するには、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) で **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 <i>vlan-id</i>	(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。
<i>cost</i>	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、STP ポート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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。STP がイネーブルになっている NNI または拡張ネットワーク インターフェイス (ENI) 上でのみスパニング ツリー コストを設定できます。ポートを NNI または ENI として設定するには、**port-type {nni | eni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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 STP ポートを設定する場合、**spanning-tree vlan *vlan-id* cost *cost*** コマンドが有効になります。

spanning-tree cost

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 gigabitethernet0/1
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	STP ポート 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。このコマンドは、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でのみ有効です。ポートを NNI または ENI として設定するには、**port-type {nni | eni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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** ステータスの場合は、**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タスを解除したり、**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
<code>errdisable recovery cause channel-misconfig</code>	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。
<code>show etherchannel summary</code>	チャンネルの EtherChannel 情報を、チャンネルグループ単位で 1 行のサマリーとして表示します。
<code>show interfaces status err-disabled</code>	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tring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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。このコマンドは、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でのみ有効です。ポートを NNI または ENI として設定するには、**port-type {nni | eni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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。

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
<code>show spanning-tree summary</code>	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。
<code>spanning-tree mst root</code>	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。
<code>spanning-tree vlan priority</code>	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 NNI に関連付けられているすべての VLAN 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、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) で **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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。STP がイネーブルになっている NNI または拡張ネットワーク インターフェイス (ENI) 上でのみスパニング ツリー ガードを設定できます。ポートを NNI または ENI として設定するには、**port-type {nni | eni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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) モードで稼働している場合は、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 NNI 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。

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 **Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット)** 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 STP インターフェイスで使用します。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 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 STP インターフェイスで使用すると、**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ことができます。

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 gigabitethernet0/2
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 gigabitethernet0/2
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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
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	STP MST ポート 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witch のプライオリティおよびタイマーを設定します。

コマンド	説明
<code>spanning-tree port-priority</code>	STP ポート プライオリティを設定します。
<code>spanning-tree vlan priority</code>	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

STP ポートのデュプレックス 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無効化し、フォワーディング ステートへの高速スパンニング ツリーの移行をイネーブルにするには、STP がイネーブルになっているネットワーク ノードインターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) 上で **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	STP ポートのリンク タイプをポイントツーポイントに指定します。
shared	STP ポートのリンク 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパンニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。STP がイネーブルになっている NNI または ENI 上でのみスパンニング ツリーのリンク タイプを設定できます。ポートを NNI または ENI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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（強制的にネイバー スイッチと再びネゴシエートさせる）します。
show spanning-tree interface <i>interface-id</i>	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 <i>interface-id</i>	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

STP がイネーブルになっているすべてのネットワーク ノード インターフェイス (NNI) または拡張 ネットワーク インターフェイス (ENI) 上でループ ガードをデフォルトでイネーブルにするには、**spanning-tree loopguard default** 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。ループ ガードをイネーブルにすると、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。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、STP がイネーブルになっている NNI または ENI でのみサ ポートされます。ポートを NNI または ENI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、 **spanning-tree** 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。

このコマンドは、ユーザ ネットワーク インターフェイス (UNI) には影響しません。

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、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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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 STP ポート上でだけ動作しま 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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
spanning-tree guard loop	指定した STP ポート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; 高速スパニング ツリー プロトコル) 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 Rapid 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) 上のスイッチでのみサポートされます。ポートを NNI または ENI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

STP は、User Network Interface (UNI; ユーザネットワーク インターフェイス) ではサポートされていません。

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。

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 PVST+ をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode 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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

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	変更箇所
12.2(53)EX	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 CGS 2520 スイッチでは、スパニング ツリー MST コンフィギュレーションは、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でのみサポートされます。ポートを NNI または ENI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

ユーザ ネットワーク インターフェイス (UNI) はスパニング ツリー プロトコル (STP) に参加しません。

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。指定できる *instance-id* の範囲は 0 ~ 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tringには表示されますが、サポートされていません。
- **revision version** : 設定のレイ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 レイジョンの設定を表示します。

MST モードでは、スイッチは最大 16 の MST インスタンスまでサポートします。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 レイ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 レイジョン番号、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、レイジョンに *region1* と名前を付けて、コンフィギュレーション レイジョンを 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。

■ spanning-tree mst configuration

関連コマンド	コマンド	説明
	<code>show spanning-tree mst configuration</code>	MST リージョンの設定を表示します。

spanning-tree mst cost

Multiple Spanning-Tree (MST) の計算に使用するパス コストを設定するには、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) で **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

<i>instance-id</i>	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。
<i>cost</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。STP がイネーブルになっている NNI または ENI 上でのみパス コストを設定できます。ポートを NNI または ENI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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 gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

■ spanning-tree mst cost

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 <i>interface-id</i>	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

<i>seconds</i>	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	変更箇所
12.2(53)EX	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 CGS 2520 スイッチでは、**spanning-tree mst configuration** は、スパニング ツリー プロトコル (STP) がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でのみサポートされます。ポートを NNI または ENI として設定するには、**port-type {nni | eni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

ユーザ ネットワーク インターフェイス (UNI) は STP に参加しません。

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 Bridge Protocol Data Unit (BPDU; ブリッジプロトコル データ ユニット) 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 が廃棄されるまでのリージョンのホップ カウントを設定します。

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 Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) 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

<i>seconds</i>	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	変更箇所
12.2(53)EX	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 CGS 2520 スイッチでは、スパニングツリー MST コンフィギュレーションは、スパニングツリープロトコル (STP) がイネーブルになっているネットワークノードインターフェイス (NNI) または拡張ネットワークインターフェイス (ENI) でのみサポートされます。ポートを NNI または ENI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

ユーザネットワークインターフェイス (UNI) は STP に参加しません。

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
<code>show spanning-tree mst</code>	MST 情報を表示します。
<code>spanning-tree mst forward-time</code>	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。
<code>spanning-tree mst max-age</code>	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。
<code>spanning-tree mst max-hops</code>	BPDU が廃棄されるまでのリージョンのホップ カウントを設定します。

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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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	変更箇所
12.2(53)EX	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 CGS 2520 スイッチでは、スパニング ツリー MST コンフィギュレーションは、スパニング ツリー プロトコル (STP) がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でのみサポートされます。ポートを NNI または ENI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

ユーザ ネットワーク インターフェイス (UNI) は STP に参加しません。

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。
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 が廃棄されるまでのリージョンのホップ カウントを設定します。

spanning-tree mst max-hops

Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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 が廃棄されるまでのリージョンのホップ カウントです。指定できるホップ カウントの範囲は 1 ~ 255 です。

デフォルト

デフォルトのホップ カウントは 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	変更箇所
12.2(53)EX	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 CGS 2520 スイッチでは、スパニング ツリー MST コンフィギュレーションは、スパニング ツリー プロトコル (STP) がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でのみサポートされます。ポートを NNI または ENI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

ユーザ ネットワーク インターフェイス (UNI) は STP に参加しません。

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 カウントを 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、STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) で **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

<i>instance-id</i>	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。
<i>priority</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされていません。STP がイネーブルになっている NNI または ENI 上でのみ MST ポート プライオリティを設定できます。ポートを ENI または NNI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

最初に選択させる STP ポート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 STP ポート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 STP ポート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。

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 gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

■ spanning-tree mst port-priority

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 <i>interface-id</i>	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	指定したスパンニング 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 Bridge Protocol Data Unit (BPDU; ブリッジプロトコル データ ユニット) 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タスは、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	変更箇所
12.2(53)EX	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せん。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 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	<i>prestandard</i> 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

指定されたスパンニング 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

<i>instance-id</i>	スパンニング 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	指定したスパンニング 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパンニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされません。STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でのみサポートされます。ポートを ENI または NNI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

例

次の例では、Multiple Spanning-Tree (MST) インスタンス 20 ~ 21 のスパンニング 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 <i>instance-id</i>	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

<i>instance-id</i>	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 Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

スパニング ツリー プロトコル (STP) は、ユーザ ネットワーク インターフェイス (UNI) ではサポートされません。STP がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) でのみサポートされます。ポートを ENI または NNI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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 が廃棄されるまでのリージョンのホップ カウントを設定します。

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、スパンニング ツリー プロトコル (STP) がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) で **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、スパンニング 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 <i>vlan-id</i>	(任意) スパンニング 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。
<i>priority</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

STP は、User Network Interface (UNI; ユーザネットワーク インターフェイス) ではサポートされていません。STP がイネーブルになっている NNI または ENI 上でのみスパンニング ツリー ポート プライオリティを設定できます。ポートを ENI または NNI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

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ンニング 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。STP ポートを 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 STP ポートを設定する場合、**spanning-tree vlan *vlan-id* port-priority *priority*** コマンドが有効になります。

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状態になる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet0/2
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)

スパニング ツリー プロトコル (STP) がイネーブルになっている PortFast 対応のネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) 上でブリッジプロトコル データ ユニット (BPDU) フィルタリングをグローバルにイネーブルにしたり、PortFast 対応 STP ポート上で BPDU ガード機能をイネーブルにしたり、すべての非トランク STP ポート上で PortFast 機能をイネーブルにしたりするには、**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 STP ポートでの 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 STP ポートを 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 STP ポート上で 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 STP ポートでの BPDU の送受信を禁止します。
bpduguard default	PortFast 対応 STP ポート上で 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 STP ポートを errdisable ステートにします。
default	すべての非トランク STP ポート上で 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、STP ポート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 NNI または ENI 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	変更箇所
	12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン STP は、スイッチ上のユーザ ネットワーク インターフェイス (UNI) ではサポートされません。スパニング ツリー設定は、STP がイネーブルになっている NNI または ENI でのみ有効です。ポートを ENI または NNI として設定するには、**port-type {eni | nni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

UNI は、通常カスタマー側のポートで、サービス プロバイダーのスパニング ツリーには参加しません。ただし、カスタマー側のポートを ENI として設定し、スパニング ツリーをイネーブルにすると、**spanning-tree guard root** 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上の

ルート ガードを設定しない限り、ENI がスパンニング ツリー ルート ポートとなる場合があります。STP がイネーブルに設定されているカスタマー側の ENI は、サービス プロバイダー側の NNI と同じスパンニング ツリーに参加します。



(注)

カスタマー側の ENI 上の STP をイネーブルにする場合、注意して使用してください。

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 STP ポート上で 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 bpdupfilter 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 STP ポートから BPDU がいくつか送信されます。スイッチ STP ポート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。PortFast 対応 STP ポート上で BPDU が受信された場合、インターフェイスは PortFast 稼動ステータスを解除され、BPDU フィルタリングはディセーブルになります。

STP ポートで **spanning-tree portfast bpdupfilter 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 bpdupfilter** 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

STP ポート上で BPDU フィルタリングをイネーブルにすると、STP ポート上でスパンニング ツリーをディセーブルにしたのと同じ結果になり、スパンニング ツリー ループが発生する可能性があります。

PortFast 動作ステータスの STP ポート上で 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 STP ポートは BPDU を受信しません。PortFast 対応 STP ポートが 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す信号が発信され、BPDU ガード機能によって STP ポートは **errdisable** ステータスになります。手動で STP ポートを再び動作させなければならないので、BPDU ガード機能は無効な設定に対する安全対策になります。サービスプロバイダー ネットワーク内でアクセス ポートがスパンニング 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、STP ポートで **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。

すべての非トランク STP ポート上で 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 STP ポートに限って設定します。そうしないと、偶発的なトポロジグループが原因でパケット 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 STP ポートは標準の転送遅延時間の経過を待たずに、ただちにスパンニング ツリー フォワーディング ステータスに移行します。

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、STP ポートで **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 STP ポート上で PortFast をディセーブルにできます。

spanning-tree portfast (グローバル コンフィギュレーション)

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 bpdudfilter 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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
spanning-tree bpdudfilter	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 STP ポートを、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)	特定の STP ポートの対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree portfast (インターフェイス コンフィギュレーション)

特定の STP ポートの対応するすべての VLAN 上で、PortFast 機能をイネーブルにするには、スパンニング ツリー プロトコル (STP) がイネーブルになっているネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) で **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、STP ポートはブロッキング 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、中間のスパンニング 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 PortFast 機能はすべてのポート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 変更箇所
	12.2(53)EX このコマンドが追加されました。

使用上のガイドライン STP は、User Network Interface (UNI; ユーザネットワーク インターフェイス) ではサポートされていません。STP がイネーブルになっている NNI または ENI 上でのみスパンニング ツリー PortFast 機能をイネーブルにできます。ポートを NNI または ENI として設定するには、**port-type {nni | eni}** 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。ENI で STP をイネーブルにするには、**spanning-tree** 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。

この機能は、エンドステーションに接続する STP ポート上でのみ使用します。そうしないと、予期しないトポロジ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) モードで稼働している場合は、その機能をイネーブルにできます。

この機能は STP ポート上のすべての VLAN に影響します。

PortFast 機能がイネーブルに設定されている NNI は、標準の転送遅延時間の経過を待たずに、ただちにスパンニング ツリー フォワーディング ステートに移行します。

spanning-tree portfast (インターフェイス コンフィギュレーション)

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 STP ポート上で 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 gigabitethernet0/2
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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
spanning-tree bpdudfilter	インターフェイスでの Bridge Protocol Data Unit (BPDU; ブリッジプロトコル データ ユニット) 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 STP ポート上で 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 STP ポートで PortFast 機能をイネーブルにします。

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 <i>seconds</i>	(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 <i>seconds</i>	(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 Bridge Protocol Data Unit (BPDU; ブリッジプロトコル データ ユニット) の間隔を設定します。指定できる範囲は 1 ~ 10 秒です。
max-age <i>seconds</i>	(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 <i>priority</i>	(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、このスイッチがルート スイッチとして選択される可能性に影響します。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 <i>net-diameter</i>	(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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

このスイッチは、ユーザ ネットワーク インターフェイス (UNI) 上のスパニング ツリー プロトコル (STP) をサポートしません。VLAN 内のスイッチ ネットワーク ノード インターフェイス (NNI) または STP がイネーブルになった拡張ネットワーク インターフェイス (ENI) だけが STP に参加します。

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。管理上ダウン状態の STP ポートは、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。

STP ポート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 STP ポート上で 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 STP ポートで 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 STP ポートの対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

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



(注) 小型フォーム ファクタ (SFP) モジュール ポートでの速度設定の制約事項については、「使用上のガイドライン」を参照してください。



(注) 小型フォーム ファクタ (SFP) モジュール ポートで速度を設定することはできませんが、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。1000BASE-T SFP モジュールが SFP モジュール スロット内にある場合の例外については、「使用上のガイドライン」を参照してください。

構文の説明

10	ポートは 10 Mb/s で稼働します。
100	ポートは 100 Mb/s で稼働します。
1000	ポートは 1000 Mb/s で稼働します。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 で稼働します (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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ファスト イーサネット ポートの速度を 10 または 100 Mb/s として設定できます。
ギガビット イーサネット ポートの速度を 10、100、または 1000 Mb/s として設定できます。
1000BASE-T SFP モジュールが SFP モジュール スロットに挿入されている場合は、速度を **nonegotiate** 以外の **10**、**100**、**1000**、または **auto** のいずれかとして設定できます。

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。

**(注)**

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 gigabitethernet0/1
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 gigabitethernet0/1
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 gigabitethernet0/1
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。

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]	<p>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。</p> <ul style="list-style-type: none"> 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]	<p>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。</p> <ul style="list-style-type: none"> 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。 <p>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せん。</p>

level pps pps [pps-low]	<p>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。</p> <ul style="list-style-type: none"> • 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 パケットのフラグ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。 <p>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せん。</p>
action { shutdown trap }	<p>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。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • 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	変更箇所
12.2(53)EX	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。

ポートがユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) の場合、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用して UNI または ENI をイネーブルにしてから、**storm-control** コマンドを使用する必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス (NNI) はデフォルトでイネーブルです。

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、Bridge Protocol Data Unit (BPDU; ブリッジプロトコル データ ユニット) 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。

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。

switchport

レイヤ 3 のモードにあるインターフェイスを、レイヤ 2 の設定のためレイヤ 2 モードに変更するには、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

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 (スイッチング) 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	変更箇所
12.2(53)EX	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。**no switchport** コマンドを入力し、ポートに IP アドレスを割り当てます。

インターフェイスが設定されている場合、ポートでスイッチング特性を設定する前に、キーワードを指定しないで **switchport** コマンドを入力してから、ポート上でスイッチング特性を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。

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。

インターフェイス上でキーワードを指定しないで **switchport** (または **no switchport**) コマンドを入力すると、影響を受けるインターフェイスの設定情報が失われ、インターフェイスがデフォルト設定に戻る可能性があります。

例

次の例では、インターフェイスをレイヤ 2 (スイッチング) ポートからレイヤ 3 (ルーテッド) ポートに変更する方法を示します。

```
Switch(config-if)# no switchport
```

次の例では、ポートをスイッチング モードに戻す方法を示します。

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

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
<code>show interfaces switchport</code>	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。
<code>show running-config</code>	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンドリファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。

switchport access vlan

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 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。スイッチポートのモードが、(`switchport mode` インターフェイス コンフィギュレーション コマンドを使用して) `access` に設定されている場合は、このコマンドを使用して、指定された VLAN のメンバとして動作するようにそのポートを設定するか、またはポートが受信する着信パケットに基づいて VLAN が割り当てられる VLAN メンバーシップ ポリシー サーバ (VMPS) プロトコルをポートが使用するよう指定します。アクセス VLAN 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

<i>vlan-id</i>	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。
dynamic	VMPS 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。スイッチは受信された新しい MAC アドレスをすべて 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。 (注) このキーワードは、ユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) 上でのみ表示されます。

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 VLAN です。

ダイナミック アクセス ポートは、最初ほどの 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	変更箇所
12.2(53)EX	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 vlan 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 6500 シリーズ スイッチなど) を設定する必要があります。

指定された VLAN が UNI-ENI コミュニティ VLAN として設定されている場合、インターフェイスは UNI-ENI コミュニティ ポートとして設定されます。そうでない場合、ポートは UNI-ENI 隔離ポートとして設定されます。

このコマンドは、IEEE802.1Q トンネル ポート上でサポートされます。

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。

- **dynamic** キーワードはネットワーク ノード インターフェイス (NNI) では表示されません。
- ソフトウェアは、Catalyst 6500 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。スイッチを VMPS サーバにすることはできません。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。
- 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 モードのレイヤ 2 インターフェイスをデフォルトの VLAN ではなく VLAN 2 で動作するように変更する方法を示します。

```
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 メンバーシップ モードを設定します。

switchport backup interface

1 組のインターフェイスで相互にバックアップする Flex Link を設定するには、スイッチのレイヤ 2 インターフェイス上で **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] {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] {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 チャンネルです。指定できる範囲は 0 ～ 48 です。
<i>interface-id</i>	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 チャンネルを指定できます。ポート チャンネル範囲は 1 ～ 486 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 ペアのプリエンブション スキームを設定します。
delay delay-time	(任意) プリエンブ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	プリエンブション 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、プリエンブションを行わないように指定します。
delay delay-time	(任意) プリエンブ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。プリエンブション モードはオフです。プリエンブションを行いません。プリエンブション遅延は 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	変更箇所
12.2(53)EX	このコマン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 fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2
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 fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preempton 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 fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preempton 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 fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 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 0/6
Switch(config-if)# switchport backup interface gigabitethernet 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 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合は、Gi0/6 が VLAN 1 ~ 50 のトラフィックを転送し、Gi0/8 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
GigabitEthernet0/6	GigabitEthernet0/8	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 Gi0/6 がダウンすると、Gi0/8 が Flex Link ペアのすべての VLAN を伝送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	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 Gi0/6 がアップになって、このインターフェイスに指定されていた VLAN がピア インターフェイス Gi0/8 上でブロックされ、Gi0/6 に転送されます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Up/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

switchport backup interface

次の例では、インターフェイス Gi0/11 にマルチキャスト高速コンバージェンスを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 0/11
Switch(config-if)# switchport backup interface gigabitEthernet 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
-----
GigabitEthernet0/11  GigabitEthernet0/12  Active Up/Backup Standby
  Preemption Mode    : off
  Multicast Fast Convergence : On
  Bandwidth          : 1000000 Kbit (Gi0/11), 1000000 Kbit (Gi0/12)
  Mac Address Move Update Vlan : auto
```

関連コマンド

コマンド	説明
show interfaces [<i>interface-id</i>] 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	変更箇所
12.2(53)EX	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せん。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。

ポートがユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) の場合、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用して UNI または ENI をイネーブルにしてから、**switchport block** コマンドを使用する必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス (NNI) はデフォルトでイネーブルです。

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。



(注)

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。

■ switchport block

例

次の例では、インターフェイス上で不明なマルチ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 multicast
```

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	変更箇所
12.2(53)EX	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、チャンネル 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 メンバーシップ 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 コマンドを使用します。モー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。

switchport mode {access | dot1q-tunnel | private-vlan | trunk}

no switchport mode

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。このキーワードは、スイッチでメトロ IP アクセス イメージまたはメトロ アクセス イメージが稼働している場合にのみサポートされます。
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ッキングします。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 **access** 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	変更箇所
12.2(53)EX	このコマン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 モードを開始すると、インターフェイスは永続的な非トランッキング モードになり、ネイバー 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ッキング 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。これらのリンク上でトランッ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、トランッキングをディセーブルにします。

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 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。



(注) 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、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。
- 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、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。



(注) ユーザネットワークインターフェイス (UNI) または拡張ネットワークインターフェイス (ENI) のみをダイナミックアクセスポートにすることができます。

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 gigabitethernet0/1
Switch(config-if)# switchport mode access
```

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 gigabitethernet0/1
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 gigabitethernet0/1
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 vlan	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。モードをデフォルトのアクセス モードにリセットするには、**no switchport mode** コマンドを使用します。

switchport mode private-vlan {host | promiscuous}

no switchport mode private-vlan



(注) **promiscuous** キーワードは、ネットワーク ノード インターフェイス (NNI) 上でだけ表示されます。

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。このキーワードは、NNI だけで使用できます。ユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) は、プライベート VLAN 混合ポートとして設定できません。

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、**access** 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	変更箇所
12.2(53)EX	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 混合ポートは NNI である必要があります。UNI または ENI を NNI として設定するには、**port-type nni** 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。

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
- NNI または ENI 用のみのポート集約プロトコル (PAgP)
- NNI または ENI 用のみの Link Aggregation Control Protocol (LACP)
- Multicast VLAN Registration (MVR; マルチキャスト VLAN レジストレーション)

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。



(注)

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。

ポートで STP がイネーブルになっている場合は、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 およびブリッジ プロトコル データ ユニット (BPDU) 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。

NNI 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)

NNI 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 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、NNI 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 gigabitethernet 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 port-security

インターフェイスで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 access**]] | **mac-address sticky** [*mac-address* | **vlan access**]] [**maximum value** [**vlan access**]]

no switchport port-security [**mac-address** *mac-address* [**vlan access**]] | **mac-address sticky** [*mac-address* | **vlan access**]] [**maximum value** [**vlan access**]]

switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

no switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

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 <i>mac-address</i>	(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 <i>vlan-id</i>	(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。
mac-address sticky [<i>mac-address</i>]	(任意) 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するには、 mac-address sticky キーワードのみを入力します。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) <i>mac-address</i> 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。 sdm prefer 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 [<i>vlan-list</i>]	(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。 <ul style="list-style-type: none"> • 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 packets 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。 <p>(注) トランク ポートに protect モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していても 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。</p>
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 packets 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、 errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、 shutdown および no shutdown 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。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ポートがユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) である場合、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用して UNI または ENI をイネーブルにしてから、**switchport port-security** コマンドを使用します。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス (NNI) はデフォルトでイネーブルです。

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せんが、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; スイッチド ポート アナライザ) の宛先ポートにすることはできません。
- 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。
- 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を解除するか、**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 コマンドを入力して手動で再びイネーブルにできます。

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済みます。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 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 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 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
```

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 <i>time</i>	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 <i>time</i> (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 <i>time</i> 期間中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	変更箇所
12.2(53)EX	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。ポートがユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) である場合、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用して UNI または ENI をイネーブルにしてから、**switchport port-security aging** コマンドを使用します。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス (NNI) はデフォルトでイネーブルです。

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 タイムを 2 時間、エージング タイプを **absolute** に設定します。

```
Switch(config)# interface gigabitethernet0/1
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 タイムを 2 分、エージング タイプを **inactivity** に設定します。

```
Switch(config)# interface gigabitethernet0/2
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 gigabitethernet0/2
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 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}
```



(注)

マッピング コマンドは、ネットワーク ノード インターフェイス (NNI) でのみサポートされます。

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。
<i>primary-vlan-id</i>	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。
<i>secondary-vlan-id</i>	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。NNI に限り、混合ポートとして設定できます。このキーワードは、ユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) ではサポートされません。
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。
<i>secondary-vlan-list</i>	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	変更箇所
12.2(53)EX	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。

混合ポートは NNI である必要があります。UNI または ENI を混合ポートとして設定することはできません。ポートを UNI として設定するには、**port-type uni** 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。

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 0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

次に、NNI をプライベート VLAN 混合ポートとして設定してそれをプライベート VLAN にマッピングする例を示します。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 gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
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。

■ switchport private-vlan

関連コマンド

コマンド	説明
<code>show interfaces private-vlan mapping</code>	<u>VLAN SVI</u> に関するプライベート VLAN マッピング情報を表示します。
<code>show vlan private-vlan</code>	スイッチに設定されているすべてのプライベート VLAN 関係またはタイプを表示します。

switchport protected

同じスイッチ上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



(注) 保護ポートは、ネットワーク ノード インターフェイス (NNI) でのみサポートされます。

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。

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	変更箇所
12.2(53)EX	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。

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 gigabitethernet0/2
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。

■ switchport protected

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 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 | native vlan vlan-id}
```

```
no switchport trunk {allowed vlan | native vlan}
```

構文の説明

allowed vlan <i>vlan-list</i>	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 <i>vlan-list</i> 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。
native vlan <i>vlan-id</i>	インターフェイスが 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。

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 ~ 4094 です。拡張範囲 VLAN (VLAN ID が 1005 より大きい) を許可 VLAN リストに追加できます。

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。

- **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 ~ 4094 です。拡張範囲 VLAN ID を使用できます。

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。

- **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

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	変更箇所
12.2(53)EX	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; ダイナミック トランキング プロトコル)、および VLAN 1 の VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル)) 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。

例

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 gigabitethernet0/2
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 gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

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 メンバーシップ モードを設定します。

switchport vlan mapping

トランク ポートに VLAN マッピングを設定するには、**switchport 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。1 対 1 の VLAN マッピング、従来の IEEE 802.1Q トンネリング (QinQ) マッピング、または選択的 QinQ マッピングを設定できます。設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
switchport vlan mapping vlan-id {translated-id | dot1q tunnel translated-id}
```

```
switchport vlan mapping default {dot1q tunnel translated-id | drop}}
```

```
no switchport vlan mapping vlan-id {translated-id | dot1q tunnel translated-id}
```

```
no switchport vlan mapping default {dot1q tunnel translated-id | drop}}
```

```
no switchport vlan mapping all
```

構文の説明

<i>vlan-id</i>	1 対 1 または選択的 QinQ マッピングに対して、有線上の VLAN と呼ばれる元の (カスタマー) VLAN (C-VLAN) を指定します。カンマで区切って複数の VLAN ID を入力したり、ハイフンで区切って一連の VLAN ID を入力することができます (1,2,3-5 など)。指定できる範囲は 1 ~ 4094 です。
<i>translated-id</i>	変換後の VLAN-ID を指定します。サービス プロバイダー ネットワークで使用される S-VLAN です。指定できる範囲は 1 ~ 4094 です。
default	指定されている以外のデフォルトを C-VLAN に指定します。
dot1q-tunnel translated-id	変換後の VLAN-ID を追加して、VLAN トンネルを指定します (外部 S-VLAN タグを追加)。S-VLAN タグの範囲は 1 ~ 4094 です。これらのキーワードを従来の QinQ マッピングに使用します。
drop	指定された C-VLAN または VLAN 以外の VLAN がドロップされるよう指定します。このキーワードは、1 対 1 または選択的 QinQ マッピングの場合に使用します。
all	no switchport vlan mapping コマンドでは、インターフェイス上のすべての VLAN マッピングが削除されるよう指定します。

デフォルト

VLAN マッピ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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスで VLAN マッピングを設定する前に、**switchport mode trunk** インターフェイス コンフィギュレーション コマンドを入力して、インターフェイスをトランク ポートとして設定します。

カスタマー ネットワークに接続されているポート上で VLAN マッピングを設定します。通常は、ユーザ ネットワーク インターフェイス (UNI) です。ただし、ネットワーク ノード インターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) で VLAN マッピングを設定することもできます。

同じ設定を使用して、物理インターフェイス上または複数のインターフェイスのポート チャンネル上で VLAN マッピングを設定できます。

VLAN マッピング タイプ :

- 1 対 1 の VLAN マッピングを設定するには、**switchport vlan mapping vlan-id translated-id** コマンドを使用します。
- インターフェイスで従来の QinQ (VLAN バンドル) を設定するには、**switchport vlan mapping default dot1q-tunnel outer vlan-id** を入力します。これは、インターフェイスをトンネル ポートとして設定し、すべての VLAN を指定された S-VLAN ID にマッピングすることと同じです。



(注) カスタマー トラフィックが混在しないようにするには、トランク ポートに従来の QinQ を設定するときに、**switchport trunk allowed vlan vlan-id** インターフェイス コンフィギュレーション コマンドを使用して、トランク ポートの許可 VLAN として外部 VLAN ID (S-VLAN) を設定する必要があります。

- インターフェイスで選択的 QinQ を設定するには、**switchport vlan mapping vlan-id dot1q-tunnel outer vlan-id** コマンドを入力します。

1 対 1 のマッピングと選択的 QinQ を同じインターフェイス上で設定できますが、両方の設定に同じ C-VLAN ID は使用できません。

1 対 1 のマッピングと選択的 QinQ の場合、指定された C-VLAN ID と S-VLAN ID の組み合わせが明示的に変換されない限り、**default drop** キーワードを使用して、トラフィックがドロップされるよう指定できます。

switchport vlan mapping コマンドの **no** 形式を使用すると、指定されたマッピング設定がクリアされます。**no switchport vlan mapping all** コマンドは、インターフェイス上のすべてのマッピング設定をクリアします。

CGS 2520 インターフェイス (VLAN マッピングが設定されている) では、S-VLAN へのマッピングがこのスイッチに入るトラフィックで発生します。したがって、VLAN マッピングが設定されているインターフェイスにその他の機能を設定するときに、VLAN ID が必要な場合は、S-VLAN ID を使用する必要があります。ただし、インターフェイス上で VLAN マッピングとイーサネット E-LMI を設定する場合を除きます。**ethernet lmi ce-vlan map vlan-id** サービス インスタンス コンフィギュレーション モード コマンドで C-VLAN を使用します。

ソース ポートがトンネル ポートとして設定されている、またはソース ポートに 1-to-2 マッピングが設定されている場合、SPAN 宛先ポートにカプセル化レプリケーションは設定できません。カプセル化レプリケーションは 1-to-1 VLAN マッピングでサポートされています。

例

次の例では、1 対 1 のマッピングを使用して、カスタマー ネットワーク内の VLAN ID 1 および 2 を、サービス プロバイダー ネットワーク内の VLAN 1001 および 1002 にマッピングし、その他のすべての VLAN ID からのトラフィックをドロップする方法を示します。

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping 1 1001
Switch(config-if)# switchport vlan mapping 2 1002
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

次の例では、従来の QinQ を使用して、ポートのすべてのトラフィックをバンドルし、S-VLAN ID が 10 のスイッチを出るようにする方法を示します。

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping default dot1q-tunnel 10
Switch(config-if)# exit
```

次の例では、5、7、または 8 の C-VLAN ID のトラフィックが、S-VLAN ID が 100 のスイッチに入るようにポート上の選択的 QinQ マッピングを設定する方法を示します。その他の VLAN ID のトラフィックはドロップされます。

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping 5, 7-8 dot1q-tunnel 100
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

関連コマンド

コマンド	説明
show vlan mapping	VLAN マッピング情報を表示します。

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 8 ~ 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 10 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	変更箇所
12.2(53)EX	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、レッドしきい値が 66 °C の場合に、イエローしきい値を 51 °C 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 °C 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	スイッチの温度ステータスおよびしきい値を表示します。

system mtu

ギガビットイーサネット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最大伝送ユニット (MTU) サイズを設定するには、**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

<i>bytes</i>	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。
<i>jumbo bytes</i>	ギガビットイーサネットポートのシステム ジャンボ フレーム サイズ (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。
<i>routing bytes</i>	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ダプタイズする最大 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ダプタイズする最大 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 に異なる値を設定した場合、設定された値は、スイッチリセットの後に適用されると、ルーテッドポートのデフォルト 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	変更箇所
12.2(53)EX	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



(注)

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。**system mtu** コマンドおよび **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 ファイルには保存されません。したがって、TFTP 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せんが、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、ギガビット イーサネット ポートの最大パケット 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 ポートおよびギガビットイーサネット ポートに設定されたパケット サイズを表示します。

table-map

Quality of Service (QoS) マッピングを作成し、テーブルマップ コンフィギュレーション モードを開始するには、**table-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。テーブル マップは、ポリシーマップ クラス **set** コマンドで指定するか、またはポリサーのマークダウン マッピングとして指定することができ、特定の packets マーキング値を別の packets マーキング値に変換するためのマッピング テーブルの作成および設定に使用できます。マッピング テーブルを削除するには、このコマンドの **no** 形式を使用します。

table-map *table-map-name*

no table-map *table-map-name*

構文の説明

class-map-name テーブル マップ名です。

デフォルト

テーブル マップ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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

作成または変更するテーブル マップの名前を指定し、テーブルマップ コンフィギュレーション モードを開始するには、このコマンドを使用します。

パケット マーキング タイプまたはカテゴリ間の *to-from* 関係を確立するために使用される変換表の一種であるマッピング テーブルを作成するには、**table-map** コマンドを使用します。たとえば、マッピング テーブルを使用して、次のカテゴリ間の *to-from* 関係を確立できます。

- サービス クラス (CoS)
- 優先順位
- Differentiated Services Code Point (DSCP; DiffServ コード ポイント)

スイッチでは、最大 256 の一意のテーブル マップをサポートしています。

テーブル マップ内の **map** 文の最大数は 64 です。

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

- **default** : テーブル マップで検出されない値を設定するためのデフォルト動作。デフォルトは次のいずれかとして指定できます。
 - *default value* : テーブル マップのデフォルト値を使用します。指定できる範囲は 0 ~ 63 です。
 - **copy** : コピーするテーブル マップで検出されない値のデフォルト動作を設定します。
 - **ignore** : 無視するテーブル マップで検出されない値のデフォルト動作を設定します。
- **exit** : QoS テーブル マップ コンフィギュレーション モードを終了します。

- **map**: *from_value* から *to_value* へのテーブル マップ。両方の値の範囲は 0～63 です。
- **no** : テーブル マップを削除するか、デフォルト値を設定します。

set コマンドでテーブル マップを指定し、これらのマップをマークダウン マッピングとして入力ポリシー マップ内のポリシーに使用できます。

テーブル マップは出力ポリシー マップでは使用できません。

例

次の例では、テーブル マップを作成して DSCP を CoS 値にマッピングし、CoS 値 4 にマッピングされていないこれらの DSCP 値を設定する方法を示します。

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 1 to 1
Switch(config-tablemap)# map from 2 to 1
Switch(config-tablemap)# map from 3 to 1
Switch(config-tablemap)# map from 4 to 2
Switch(config-tablemap)# map from 5 to 2
Switch(config-tablemap)# map from 6 to 3
Switch(config-tablemap)# default 4
Switch(config-tablemap)# exit
```

show table 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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
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 cos	パケットに CoS、DSCP、IP precedence、または QoS グループ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 table-map	QoS テーブル マップを表示します。

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*



(注) TDR は、Cisco CGS 2520 スイッチの銅線のイーサネット 10/100 または 10/100/1000 ポートでのみサポートされます。これには、RJ-45 コネクタを使用して 10/100/1000 ポートとして設定されるデュアル パーパス ポートが含まれます。

構文の説明

<i>interface-id</i>	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	変更箇所
12.2(53)EX	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 機能を使用すると、ケーブル配線の問題を診断して解決できます。TDR は、銅線のイーサネット 10/100 または 10/100/1000 ポートでのみサポートされます。小型フォーム ファクタ (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 gigabitethernet0/2
TDR test started on interface Gi0/2
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 gigabitethernet0/3
TDR test on Gi0/9 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

■ test cable-diagnostics tdr

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

指定された送信元 MAC アドレスから指定された宛先 MAC アドレスまでのパケットがたどるレイヤ 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]
```



(注) レイヤ 2 traceroute は、ネットワーク ノード インターフェイス (NNI) 上でだけ使用できます。

構文の説明

interface <i>interface-id</i>	(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 <i>vlan-id</i>	(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	変更箇所
12.2(53)EX	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。



(注) レイヤ 2 traceroute は、NNI 上でだけ使用できます。

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。

パス内で識別可能なホップ カウントは 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 **tracert** 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# tracert mac 0000.00bb.bbbb 0000.00aa.aaaa
Source 0000.00bb.bbbb found on CGS-2520-16S-8PC
1 CGS-2520-16S-8PC (77.77.77.77) : Fa0/21 => Fa0/22
Destination 0000.00aa.aaaa found on CGS-2520-16S-8PC
Layer2 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# tracert mac 0000.00bb.bbbb 0000.00aa.aaaa detail
Source 0000.00bb.bbbb found on CGS-2520-16S-8PC (77.77.77.77)
1 CGS-2520-16S-8PC / 77.77.77.77 :
    Fa0/21 [auto, auto] => Fa0/22 [auto, auto]
Destination 0000.00aa.aaaa found on CGS-2520-16S-8PC (77.77.77.77)
Layer2 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# tracert mac interface fastethernet0/21 0000.00bb.bbbb interface
fastethernet0/22 0000.00aa.aaaa
Source 0000.00bb.bbbb found on CGS-2520-16S-8PC
1 CGS-2520-16S-8PC (77.77.77.77) : Fa0/21 => Fa0/22
Destination 0000.00aa.aaaa found on CGS-2520-16S-8PC
Layer2 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# tracert mac 0000.00bb.bbbb 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.00bb.bbbb found on con5[CGS-2520-16S-8PC] (77.77.77.77)
con5 / CGS-2520-16S-8PC/ 77.77.77.77 :
    Fa0/18 [auto, auto] => Fa 0/21 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 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# tracert 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# tracert 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。

tracert mac ip

指定された送信元 IP アドレスまたはホスト名から指定された宛先 IP アドレスまたはホスト名までのパケットがたどるレイヤ 2 パスを表示するには、**tracert mac ip** 特権 EXEC コマンドを使用します。

```
tracert mac ip {source-ip-address | source-hostname} {destination-ip-address |
destination-hostname} [detail]
```



(注)

レイヤ 2 tracert は、ネットワーク ノード インターフェイス (NNI) 上でだけ使用できます。

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	変更箇所
12.2(53)EX	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 tracert 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。



(注)

レイヤ 2 tracert は、ネットワーク ノード インターフェイス (NNI) 上でだけ使用できます。

スイッチがレイヤ 2 パス内でレイヤ 2 tracert 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。

パス内で識別可能なホップ カウントは 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、**tracert 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[CGS-2520-24TC] (2.2.6.6)
con6 / CGS-2520-24TC/ 2.2.6.6 :
    Fa0/10 [auto, auto] => Fa0/14 [auto, auto]
con3 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 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) :Fa0/10 => Fa0/14
con3          (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
shutdown	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。

udld

UniDirectional Link Detection (UDLD; 単方向リンク検出) 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 <i>message-timer-interval</i>	アダプタイズ 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 7 ~ 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 60 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

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 リンクの単方向トラフィックによる単方向リンク、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」の項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となります。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します。

- **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	変更箇所
12.2(53)EX	このコマンドが追加されました。

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。ポートがユーザ ネットワーク インターフェイス (UNI) または拡張ネットワーク インターフェイス (ENI) の場合、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用して UNI または ENI をイネーブルにしてから、**udld port** コマンドを使用する必要があります。UNI と ENI は、デフォルトでディセーブルに設定されています。ネットワーク ノード インターフェイス (NNI) はデフォルトでイネーブルです。

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。

スイッチ ソフトウェアが小型フォーム ファクタ (SFP) モジュール変更を検出し、ポートが光ファイバから非光ファイバ (またはその逆) に変更される場合、すべての設定は維持されます。

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します。

- **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 gigabitethernet0/1
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 gigabitethernet0/1
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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
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。

コマンド	説明
<code>udld</code>	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。
<code>udld reset</code>	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

単方向リンク検出 (UDLD) 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 (イーサネットの場合には、スパニング ツリー、ポート集約プロトコル (PAgP) などの他の機能を介することで有効になります)。

udld reset



(注) PAgP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

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	変更箇所
12.2(53)EX	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	動作設定を表示します。構文情報については、Cisco IOS Release 12.2 のコマンド リファレンス一覧ページへアクセスする次のリンクを使用します。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html 「Cisco IOS Commands Master List, Release 12.2」を選択して、コマンドの項目へ移動します。
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。

コマンド	説明
<code>udld</code>	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。
<code>udld port</code>	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 <code>udld</code> 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。

uni count

イーサネット仮想接続 (EVC) のユーザネットワーク インターフェイス (UNI) カウントを設定するには、**uni count** EVC 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。

uni count value [multipoint]

no uni count

構文の説明

value	EVC の UNI の数を設定します。指定できる範囲は 1 ~ 1024 です。デフォルトは 2 です。
multipoint	(任意) ポイントツーマルチポイント サービスを選択します。このキーワードは、 uni count 値に 2 を入力した場合にのみ表示されます。 <ul style="list-style-type: none">値を入力しない場合、または 1 や 2 を入力した場合、サービスはデフォルトでポイントツーポイントサービスになります。2 を入力した場合、ポイントツーマルチポイント サービスを設定できます。uni count の値に 3 以上を入力した場合、サービスはポイントツーマルチポイントです。

デフォルト

デフォルトの UNI カウントは 2 です。UNI カウントを入力しない場合のデフォルト サービスはポイントツーマルチポイントです。

コマンド モード

EVC コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

UNI カウントは、EVC のタイプ オブ サービスを決定します。

- コマンドを入力しない場合、UNI カウントはデフォルトで 2 になり、サービスはデフォルトでポイントツーポイント サービスになります。
- 手動で値 2 を入力した場合、サービスをデフォルトのままにするか、**multipoint** キーワードを入力してポイントツーマルチポイント サービスを設定できます。
- 3 以上の値を入力すると、サービスはポイントツーマルチポイント サービスとなります。

ドメイン内の **Maintenance End Point (MEP; メンテナンス エンド ポイント)** の正しい数を知っておく必要があります。実際のエンドポイントの数よりも大きい UNI カウントの値を入力した場合、すべてのエンドポイントが動作中であっても、UNI ステータスは部分的にアクティブと表示されます。実際のエンドポイントの数よりも少ない UNI カウントを入力した場合、すべてのエンドポイントが動作中でなくても、UNI ステータスはアクティブと表示されます。

**注意**

UNI カウントの設定は、設定されたカウントよりも多くのエンドポイントを設定することを妨げるものではありません。たとえば、UNI カウントを 5 に設定したが、10 個の MEP を作成した場合、ステータスを部分的にアクティブに変更することなく、ドメイン内の任意の 5 個の MEP を停止できます。

例

次の例では、UNI カウントが 2 のポイントツーマルチポイント サービスを設定します。

```
Switch(config)# ethernet evc test1
Switch(config-etc)# uni count 2 multipoint
```

関連コマンド

コマンド	説明
ethernet evc evc-id	EVC を定義し、EVC コンフィギュレーション モードを開始します。

uni-vlan

VLAN を User Network Interface-Enhanced Network Interface (UNI-ENI) コミュニティ VLAN または隔離 VLAN として設定するには、**uni-vlan** VLAN コンフィギュレーション コマンドを使用します。コミュニティ VLAN に割り当てられたスイッチ上の UNI および ENI は、相互にパケットを交換できません。隔離 VLAN 内の UNI および ENI はパケットを交換できません。VLAN をデフォルトの UNI-ENI 隔離 VLAN に戻すには、このコマンドの **no** 形式を使用します。

uni-vlan {community | isolated}

no uni-vlan

構文の説明

community	UNI-ENI VLAN をコミュニティ VLAN として指定します。
isolated	UNI-ENI VLAN を隔離 VLAN として指定します。

デフォルト

デフォルトの VLAN 設定は UNI-ENI 隔離 VLAN です。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

UNI-ENI 隔離 VLAN では、パケットは VLAN 内の UNI または ENI 間で交換されません。パケットは、同じ UNI 隔離 VLAN 内の UNI や ENI とネットワーク ノード インターフェイス (NNI) との間で交換できます。

UNI-ENI コミュニティ VLAN では、パケットは同じコミュニティ VLAN 内の UNI 間、ENI 間、または UNI と NNI 間で交換できます。ただし、UNI コミュニティ VLAN 内では、UNI と ENI の組み合わせ合計が 8 を超えることはできません。



(注)

ローカル スイッチングは、同一コミュニティ VLAN の ENI および UNI との間で行われます。スパンニング ツリーは UNI ではなく ENI でイネーブルに設定できるため、同一コミュニティ VLAN で ENI および UNI を設定する場合は注意が必要です。UNI は常に、フォワーディング ステートです。

VLAN 1 は常に UNI-ENI 隔離 VLAN です。VLAN 1 を UNI-ENI コミュニティ VLAN として設定できません。予約 VLAN 1002 ~ 1005 は、イーサネット VLAN ではありません。

他の VLAN と同様に、**switchport access vlan *vlan-id*** インターフェイス コンフィギュレーション コマンドを使用して、UNI-ENI VLAN にポートを静的に割り当てることができます。また、ポートは UNI-ENI VLAN に動的に割り当てられます。

uni-vlan コマンドは、VLAN コンフィギュレーション モードを終了するまで有効になりません。

UNI-ENI VLAN をリモート スイッチド ポート アナライザ (RSPAN) VLAN にすることはできません。

UNI-ENI VLAN をプライベート VLAN にすることはできません。

UNI-ENI 隔離 VLAN を RSPAN VLAN またはプライベート VLAN に変更するには、**rspan-vlan** または **private-vlan** VLAN コンフィギュレーション コマンドを入力します。これにより、デフォルトの隔離 VLAN 設定が上書きされます。UNI-ENI コミュニティ VLAN を RSPAN VLAN またはプライベート VLAN に変更するには、最初に **no uni-vlan** VLAN コンフィギュレーション コマンドを入力してデフォルトの UNI-ENI 隔離 VLAN コンフィギュレーションに戻してから、**rspan-vlan** または **private-vlan** VLAN コンフィギュレーション コマンドを入力します。



(注)

UNI-ENI VLAN とその他の機能との相互作用の詳細については、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 20 をデフォルトの UNI-ENI 隔離 VLAN から UNI-ENI コミュニティ VLAN に変更する方法を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# uni-vlan community
Switch(config-vlan)# exit
```

設定を確認するには、**show vlan uni-vlan** または **show vlan *vlan-id* uni-vlan [type]** 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 uni-vlan	スイッチ上の UNI-ENI VLAN を表示します。

violate-action

認定情報レート（CIR）または最大情報レート（PIR）に関して、パケットが適合レートに超過バーストを加えたレートよりも大きいレートの場合にポリシーマップクラスの複数のアクションを設定するには、**violate-action** ポリシーマップクラス ポリシング コンフィギュレーション コマンドを使用します。アクションをキャンセルしたり、デフォルトアクション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。

```
violate-action {drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table
table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence]
[table table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp |
precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit}}
```

```
no violate-action {drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence]
[table table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp |
precedence] [table table-map name]} | set-prec-transmit {new-precedence-value |
[cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value
| transmit}}
```

構文の説明

drop	パケットをドロップします。
set-cos-transmit <i>new-cos-value</i>	パケットの新しいサービスクラス（CoS）値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 CoS 値に指定できる範囲は 0 ～ 7 です。
set-dscp-transmit <i>new-dscp-value</i>	パケットの新しい DiffServ コードポイント（DSCP）値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 DSCP 値に指定できる範囲は 0 ～ 63 です。
set-prec-transmit <i>new-precedence-value</i>	パケットの新しい IP precedence 値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 IP precedence 値に指定できる範囲は 0 ～ 7 です。
set-qos-transmit <i>qos-group-value</i>	パケットの新しい Quality of Service（QoS）グループ値を設定し、パケットを送信します。これにより、マーキングアクションの <i>to-type</i> が指定されます。新規 QoS 値に指定できる範囲は 0 ～ 99 です。
cos	(任意) 着信パケットの CoS 値に基づき上記のキーワードに指定されているパケットマーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
dscp	(任意) 着信パケットの DSCP 値に基づき上記のキーワードに指定されているパケットマーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
precedence	(任意) 着信パケットの IP precedence 値に基づき上記のキーワードに指定されているパケットマーキングを設定し、パケットを送信します。これにより、拡張パケットマーキングアクションの <i>from-type</i> が指定されます。
table table-map name	(任意) 上記の <i>from-type</i> キーワードとともに使用します。拡張パケットマーキングに使用するテーブルマップを指定します。このテーブルマップを使用して、アクションの <i>from-type</i> パラメータに基づき、アクションの <i>to-type</i> がマーキングされます。
transmit	(任意) パケットを変更せずに送信します。

デフォルト

デフォルトのアクションは、パケットのドロップです。

コマンド モード ポリシーマップ クラス ポリシング設定

コマンド履歴	リリース	変更箇所
	12.2(53)EX	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 レートが、認定情報レートと最大情報レートに関して適合レートに超過バーストを加えたレートよりも大きい場合に、パケットの違反アクションを設定します。

適合アクションが **drop** に設定されている場合、超過アクションおよび違反アクションは自動的に **drop** に設定されます。超過アクションが **drop** に設定されている場合、違反アクションは自動的に **drop** に設定されます。

パケットを変更せずに送信し、明示的な値を使用してマーキングし、拡張パケット マーキングのすべての組み合わせを使用するように違反アクションを設定できます。拡張パケット マーキングによって、あらゆる着信 QoS マーキングおよびテーブル マップに基づく QoS マーキングが変更されます。また、スイッチは、同じクラスに対する複数の QoS パラメータのマーキングや、適合アクション、超過アクション、および違反アクションのマーキングの同時設定もサポートします。

ポリシーマップ クラス ポリシング コンフィギュレーション モードにアクセスするには、**police** ポリシーマップ クラス コマンドを入力します。詳細については、**police** コマンドを参照してください。

トラフィック クラスに 1 つ以上の違反アクションを設定するには、このコマンドを使用します。

個別ポリサーおよび集約ポリサーの両方について違反アクションを設定しない場合は、デフォルトで違反クラスが超過アクションと同じアクションに割り当てられます。

例

次の例では、情報レートを 23000 ビット/秒 (b/s)、バースト レートを 10000 b/s に設定するポリシーマップで複数のアクションを設定する方法を示します。

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 23000 10000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-prec-transmit prec table
policed-prec-table-map-name
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# 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	指定したクラスマップ名のトラフィック分類一致基準を定義します。
conform-action	CIR に適合するトラフィックに対して実行するアクションを定義します。
exceed-action	適合レートと、適合レートに超過バーストを加えたレートとの間のトラフィックで実行されるアクションを定義します。
police	分類したトラフィックにポリサーを定義します。

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	Quality of Service (QoS) ポリシー マップを表示します。

vlan

VLAN を追加して VLAN コンフィギュレーション モードを開始するには、VLAN ID を指定して **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 を削除する場合は、このコマンドの **no** 形式を使用します。標準範囲 VLAN (VLAN ID 1 ~ 1005) の設定情報は、常に VLAN データベースおよびコンフィギュレーション ファイルを実行しているスイッチに保存されます。拡張範囲 VLAN (VLAN ID が 1005 よりも大きい) の設定情報は、コンフィギュレーション ファイルを実行しているスイッチのみに保存されます。**copy running-config startup-config** 特権 EXEC コマンドを使用すれば、スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存できます。

vlan *vlan-id*

no vlan *vlan-id*

構文の説明

<i>vlan-id</i>	追加および設定する VLAN の ID。 <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。1 つの VLAN ID、それぞれをカンマで区切った一連の VLAN ID、またはハイフンを間に挿入した VLAN ID の範囲を入力できます。
----------------	--

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

拡張範囲 VLAN (VLAN ID 1006 ~ 4094) は VLAN データベースに追加されませんが、すべての VLAN コンフィギュレーションは実行コンフィギュレーションに保存され、これをスイッチ 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ことができます。

vlan コマンドを VLAN ID を指定して入力すると、VLAN 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。無効な VLAN ID を入力すると、エラー メッセージが表示され、VLAN コンフィギュレーション モードを開始できません。

既存の VLAN の VLAN ID を入力すると、新しい VLAN は作成されませんが、その VLAN の VLAN パラメータを変更できます。指定された VLAN は、VLAN コンフィギュレーション モードを終了したときに追加または変更されます。(VLAN 1 ~ 1005 の) **shutdown** コマンドだけがただちに有効になります。

次のコンフィギュレーション コマンドを VLAN コンフィギュレーション モードで利用できます。各コマンドの **no** 形式を使用すると、特性がそのデフォルト ステートに戻ります。



(注)

すべてのコマンドが表示されますが、拡張範囲 VLAN でサポートされる VLAN コンフィギュレーション コマンドは、**mtu mtu-size**、**private-vlan**、**remote-span**、および **uni-vlan** だけです。拡張範囲 VLAN の場合、他のすべての特性はデフォルト ステートのままにしておく必要があります。



(注)

スイッチは、イーサネット VLAN だけをサポートしています。FDDI およびトークンリング VLAN のパラメータを設定して、vlan.dat ファイルでの結果を表示できますが、これらのパラメータは使用されません。

- **are are-number** : TrCRF VLAN の全ルート エクスプローラ (ARE) ホップの最大数を定義します。指定できる範囲は 0 ~ 13 です。デフォルトは 7 です。
- **backupcrf {enable | disable}**: TrCRF VLAN のバックアップ CRF モードを指定します。
- **bridge {bridge-number| type}** : 論理分散ソース ルーティングブリッジ、つまり、FDDI-NET、トークンリング NET、および TrBRF VLAN 内で親 VLAN としてこの VLAN を持つすべての論理リングと相互接続するブリッジを指定します。指定できる範囲は 0 ~ 15 です。デフォルトのブリッジ番号は 0 です。
- **exit** : 変更を適用し、VLAN データベース リビジョン番号 (VLAN 1 ~ 1005 だけ) を増加させ、VLAN コンフィギュレーションモードを終了します。
- **media** : VLAN メディア タイプを定義します。
 - **ethernet** は、イーサネット メディア タイプです (デフォルト)。
 - **fddi** は、FDDI メディア タイプです。
 - **fd-net** は、FDDI Network Entity Title (FDDI-NET) メディア タイプです。
 - **tokenring** は、トークンリング メディア タイプまたは TrCRF です。
 - **tr-net** は、トークンリング Network Entity Title (NET) メディア タイプまたは TrBRF メディア タイプです。
- **mtu mtu-size** : Maximum Transmission Unit (MTU; 最大伝送ユニット) (バイト単位のパケットサイズ) を指定します。指定できる範囲は 1500 ~ 18190 です。デフォルトは 1500 バイトです。
- **name vlan-name** : 管理ドメイン内で一意である 1 ~ 32 文字の ASCII 文字列で VLAN を命名します。デフォルトは VLANxxxx です。ここで、xxxx は VLAN ID 番号と同じ 4 桁の数字 (先行ゼロを含む) です。
- **no** : コマンドを無効にし、デフォルト設定に戻します。
- **parent parent-vlan-id** : 既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定します。指定できる範囲は 0 ~ 1005 です。デフォルトの親 VLAN ID は 0 (親 VLAN なし) です。
- **private-vlan** : VLAN をプライベート VLAN のコミュニティ、隔離、またはプライマリ VLAN として設定します。または、プライベート VLAN のプライマリとセカンダリ VLAN 間にアソシエーションを設定します。詳細については、**private-vlan** コマンドを参照してください。
- **remote-span** : VLAN を Remote Switched Port Analyzer (RSPAN; リモート スイッチド ポートアナライザ) VLAN として設定します。RSPAN 機能が既存の VLAN に追加される場合、まず VLAN は削除され、次に RSPAN 機能とともに再生されます。RSPAN 機能が削除されるまで、どのアクセス ポートも非アクティブになります。ラーニングは VLAN 上でディセーブルになります。詳細については、**remote-span** コマンドを参照してください。
- **ring ring-number** : FDDI、トークンリング、または TrCRF VLAN の論理リングを定義します。指定できる範囲は 1 ~ 4095 です。
- **said said-value** : IEEE 802.10 に記載されている Security Association Identifier (SAID) を指定します。指定できる ID は、1 ~ 4294967294 です。この数字は、管理ドメイン内で一意である必要があります。デフォルト値は、100000 に VLAN ID 番号を加算した値です。

- **shutdown** : VLAN 上で VLAN スイッチングをシャットダウンします。このコマンドはただちに有効になります。他のコマンドは、VLAN コンフィギュレーション モードを終了したときに有効になります。
- **state** : VLAN ステートを指定します。
 - **active** は、VLAN が稼動中であることを意味します (デフォルト)。
 - **suspend** は、VLAN が停止していることを意味します。停止している VLAN はパケットを通過させません。
- **ste *ste-number*** は、TrCRF VLAN のスパニング ツリー エクスプローラ (STE) ホップの最大数を定義します。指定できる範囲は 0 ~ 13 です。デフォルトは 7 です。
- **stp type** : FDDI-NET、トークンリング NET、または TrBRF VLAN のスパニング ツリー タイプを定義します。
 - Source-Route Transparent (SRT; ソースルート トランスペアレント) ブリッジングを実行している IEEE イーサネット STP の場合は、**ieec**
 - Source-Route Bridge (SRB; ソースルートブリッジ) を実行している IBM STP の場合は、**ibm**
 - Source-Route Transparent (SRT; ソースルート トランスペアレント) ブリッジング (IEEE) および Source-Route Bridge (SRB) (IBM) の組み合わせを実行している STP の場合は、**auto**
- **tb-vlan1 *tb-vlan1-id*** および **tb-vlan2 *tb-vlan2-id*** : この VLAN にトランスレーショナルブリッジングが行われている 1 番めおよび 2 番めの VLAN を指定します。トランスレーショナル VLAN は、たとえば FDDI またはトークンリングをイーサネットに変換します。指定できる範囲は 0 ~ 1005 です。値が指定されないと、0 (トランスレーショナルブリッジングなし) と見なされます。
- **uni-vlan {community | isolated}** : User Network Interface-Enhanced Network Interface (UNI-ENI) コミュニティ VLAN または UNI-ENI 隔離 VLAN として VLAN を設定します。コミュニティ VLAN に割り当てられたスイッチ上の複数の UNI は、互いに通信できます。UNI-ENI VLAN が独立 (デフォルト) の場合、VLAN 内のポートは通信できません。詳細については、**uni count** コマンドを参照してください。

例

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには *VLANxxx* の *vlan-name* が含まれています。ここで、*xxxx* は VLAN ID 番号と同じ 4 桁の数字 (先行ゼロを含む) です。デフォルトの **media** オプションは **ethernet** です。**state** オプションは **active** です。デフォルトの *said-value* 変数は、100000 に VLAN ID を加算した値です。*mtu-size* 変数は 1500、**stp-type** オプションは **ieec** です。**exit** VLAN コンフィギュレーション コマンドを入力すると、VLAN がない場合は追加されます。それ以外の場合、このコマンドによる影響はありません。

次の例では、すべての特性をデフォルトで新しい VLAN を作成し、**config-vlan** モードを開始する方法を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
```

次の例では、新しい拡張範囲の VLAN を作成し、VLAN コンフィギュレーション モードを開始して VLAN を UNI-ENI コミュニティ VLAN として設定し、この新しい VLAN をスイッチ 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方法を示します。

```
Switch(config)# vlan 2000
Switch(config-vlan)# uni-vlan community
Switch(config-vlan)# exit
Switch(config)# exit
Switch# copy running-config startup config
```

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
show vlan	すべての設定された VLAN または 1 つの VLAN (VLAN ID または名前が指定されている場合) のパラメータを表示します。

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

<i>name</i>	VLAN マップ名
<i>number</i>	(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	変更箇所
12.2(53)EX	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。



(注)

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 dot1q tag native

すべての IEEE 802.1Q トランク ポートでネイティブ VLAN フレームのタグ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

このコマンドは、スイッチでメトロ アクセス イメージまたはメトロ IP アクセス イメージが稼動している場合にのみサポートされます。

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。

デフォルト

IEEE 802.1Q ネイティブ VLAN タグ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	変更箇所
12.2(53)EX	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 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 802.1Q トランク ポートから出るネイティブ VLAN パケットはタグ付けされません。

このコマンドを 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 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 802.1Q トランクで伝送される可能性があります。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 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。



(注)

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 802.1Q タグ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	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** 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。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

<i>mapname</i>	VLAN マップ エントリ名
<i>list</i>	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	変更箇所
12.2(53)EX	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らないように、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。



(注)

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	変更箇所
12.2(53)EX	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	<i>interval</i>	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	変更箇所
	12.2(53)EX	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

<i>count</i>	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	変更箇所
12.2(53)EX	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。

vmmps 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、**vmmps 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。

vmmps server *ipaddress* [**primary**]

no vmmps server [*ipaddress*]

構文の説明

<i>ipaddress</i>	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	変更箇所
12.2(53)EX	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。

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ず。

```
Switch(config)# vmmps server 191.10.49.20 primary
Switch(config)# vmmps server 191.10.49.21
Switch(config)# vmmps 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 vmmps server 191.10.49.21
```

設定を確認するには、**show vmmps** 特権 EXEC コマンドを入力して、VMPS Domain Server 列を調べます。

■ vmps server

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。



APPENDIX 3

Cisco CGS 2520 スイッチ Debug コマンド

この付録では、Cisco CGS 2520 スイッチで使用するため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 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。

コマンド 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	変更箇所
12.2(53)EX	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 backup コマンドは、**no debug backup** コマンドと同じです。

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 dot1x

IEEE 802.1x 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 | packets | registry | state-machine}
```

```
no debug dot1x {all | errors | events | packets | registry | state-machine}
```

構文の説明

all	すべての IEEE 802.1x 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。
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。

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	変更箇所
12.2(53)EX	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。

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 etherchannel

EtherChannel/PAgP 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; ポート集約プロトコル) 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**]



(注)

PAgP を使用できるのは、ネットワーク ノードインターフェイス (NNI) または拡張ネットワーク インターフェイス (ENI) 上だけです。

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tring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	変更箇所
12.2(53)EX	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。

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	チャンネルの EtherChannel 情報を表示します。

debug ethernet service

イーサネット カスタマーサービス インスタンスのデバッグをイネーブルにするには、**debug ethernet service** 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 ethernet service {all | api | error | evc [id evc-id] | instance [id id interface-id |
interface interface-id] | interface [interface-id] | oam-mgr}
```

```
no debug ethernet service {all | api | error | evc [id evc-id] | instance [id id interface-id |
interface interface-id] | interface [interface-id] | oam-mgr}
```

構文の説明

all	イーサネット カスタマーサービスのデバッグ メッセージをすべて表示します。
api	イーサネット インフラストラクチャとクライアントとの相互作用に関するデバッグメッセージを表示します。
error	イーサネット インフラストラクチャ サブシステムで発生したイーサネット カスタマーサービスのエラー メッセージを表示します。
evc	Ethernet Virtual Connection (EVC; イーサネット仮想接続) のデバッグ メッセージを表示します。
id evc-id	(任意) 特定の EVC ID に関連する EVC デバッグ メッセージを表示します。EVC ID に設定できる文字列は 1 ~ 100 文字です。
instance	イーサネット カスタマーサービス インスタンスに関連するデバッグ メッセージを表示します。
id id interface-id	(任意) 特定のイーサネットのサービス インスタンス ID およびインターフェイスに対するイーサネット サービス インスタンスのデバッグ メッセージを表示します。サービス ID に指定できる範囲は 1 ~ 4294967295 です。インターフェイスは物理インターフェイスです。
interface interface-id	(任意) instance キーワードの後に入力すると、インターフェイスのサービス インスタンス デバッグ メッセージが表示されます。ここでは、インターフェイス ID を入力する必要があります。
interface [interface-id]	すべてのインターフェイスまたは指定したインターフェイスにおけるイーサネット サービスのデバッグを表示します。
oam-mgr	インフラストラクチャのイーサネット Operation, Administration, and Maintenance (OAM; 運用管理および保守) マネージャ コンポーネントに対するデバッグ メッセージを表示します。

コマンド デフォルト

イーサネット サービスの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	変更箇所
12.2(53)EX	このコマンドが追加されました。

■ debug ethernet service

使用上のガイドライン **undebug ethernet service** コマンドは、**no debug ethernet service** コマンドと同じです。

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 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

<i>interface-id</i>	タイプ スイッチ番号/モジュール番号/ポート (例 : gigabitethernet 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 <i>interface-number</i>	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。 <i>interface-number</i> は常に 0 です。
port-channel <i>port-channel-number</i>	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。 <i>port-channel-number</i> は 1 ~ 48 です。
vlan <i>vlan-id</i>	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 <i>vlan id</i> 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	変更箇所
12.2(53)EX	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。

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	チャンネルの 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

<i>mac-address</i>	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	変更箇所
12.2(53)EX	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。

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	変更箇所
12.2(53)EX	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。

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	変更箇所
12.2(53)EX	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。

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	変更箇所
12.2(53)EX	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 snooping コマンドは、**no debug ip igmp snooping** コマンドと同じです。

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 ip sla error twamp connection

Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) のデバッグ出力をイネーブルにするには、**debug ip sla error twamp connection** コマンドを特権 EXEC モードで使用します。このデバッグ出力は、TWAMP クライアントとサーバとの通信中に発生する例外を示します。デバッグ出力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 sla error twamp connection [source-ip ip-address]

no debug ip sla error twamp connection [source-ip ip-address]

構文の説明

source-ip ip-address (任意) 指定したソースの IP Performance Metrics (IPPM; IP パフォーマンスメトリック) TWAMP 接続をデバッグします。クライアントデバイスの IP アドレスを使用するソースを指定します。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

debug ip sla error twamp connection 特権 EXEC コマンドでは、サーバとリフレクタとの TWAMP 通信中に発生した例外に関するメッセージが表示されます。

undebug ip sla error twamp connection コマンドは、**no debug ip sla error twamp connection** コマンドと同じです。



(注)

debug ip sla error twamp connection コマンドではデバッグ出力が比較的少なく生成されるため、**debug ip sla trace twamp connection** コマンドを使用する前に、**debug ip sla error twamp connection** コマンドを使用します。

debug ip sla error twamp connection コマンドは IPv4 ネットワークでサポートされます。

関連コマンド

コマンド	説明
debug ip sla error twamp control reflector	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp control server	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp session	IP SLA TWAMP 送信元とリフレクタとの通信中に起こる例外を表示します。
debug ip sla trace twamp connection	IP SLA TWAMP クライアントとサーバ間の正常な通信を表示します。

debug ip sla trace twamp control reflector	IP SLA TWAMP リフレクタによって送信された TWAMP サーバへの正常な通信を表示します。
debug ip sla trace twamp control server	IP SLA TWAMP サーバによって送信された TWAMP リフレクタへの正常な通信を表示します。
debug ip sla trace twamp session	IP SLA TWAMP 送信元とリフレクタ間の正常な通信を表示します。
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 ip sla error twamp control reflector

Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) のデバッグ出力をイネーブルにするには、**debug ip sla error twamp control reflector** コマンドを特権 EXEC モードで使用します。このデバッグ出力は、TWAMP サーバとリフレクタとの通信中に発生する例外を示します。デバッグ出力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 sla error twamp control reflector

no debug ip sla error twamp control reflector

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

debug ip sla error twamp control reflector 特権 EXEC コマンドでは、TWAMP セッション リフレクタから TWAMP セッション サーバへの通信中に発生した例外に関するメッセージが表示されます。



(注)

debug ip sla error twamp control reflector コマンドではデバッグ出力が比較的少なく生成されるため、**debug ip sla trace twamp control reflector** コマンドを使用する前に、**debug ip sla error twamp control reflector** コマンドを使用します。

debug ip sla error twamp control reflector コマンドは IPv4 ネットワークでサポートされます。

undebug ip sla error twamp control reflector コマンドは、**no debug ip sla error twamp control reflector** コマンドと同じです。

関連コマンド

コマンド	説明
debug ip sla error twamp connection	IP SLA TWAMP クライアントとサーバとの通信中に起こる例外を表示します。
debug ip sla error twamp control server	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp session	IP SLA TWAMP 送信元とリフレクタとの通信中に起こる例外を表示します。
debug ip sla trace twamp connection	IP SLA TWAMP クライアントとサーバ間の正常な通信を表示します。
debug ip sla trace twamp control reflector	IP SLA TWAMP リフレクタによって送信された TWAMP サーバへの正常な通信を表示します。

debug ip sla trace twamp control server	IP SLA TWAMP サーバによって送信された TWAMP リフレクタへの正常な通信を表示します。
debug ip sla trace twamp session	IP SLA TWAMP 送信元とリフレクタ間の正常な通信を表示します。
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 ip sla error twamp control server

TWAMP サーバとリフレクタとの通信中に発生する Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) 例外のデバッグ出力をイネーブルにするには、**debug ip sla error twamp control server** コマンドを特権 EXEC モードで使用します。デバッグ出力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 sla error twamp control server

no debug ip sla error twamp control server

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

debug ip sla error twamp control server 特権 EXEC コマンドでは、TWAMP セッション サーバから TWAMP セッション リフレクタへの通信中に発生した例外に関するメッセージが表示されます。



(注)

debug ip sla error twamp control server コマンドではデバッグ出力が比較的少なく生成されるため、**debug ip sla trace twamp control server** コマンドを使用する前に、**debug ip sla error twamp control server** コマンドを使用します。

debug ip sla error twamp control server コマンドは IPv4 ネットワークでサポートされます。

undebug ip sla error twamp control server コマンドは、**no debug ip sla error twamp control server** コマンドと同じです。

関連コマンド

コマンド	説明
debug ip sla error twamp connection	IP SLA TWAMP クライアントとサーバとの通信中に起こる例外を表示します。
debug ip sla error twamp control reflector	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp session	IP SLA TWAMP 送信元とリフレクタとの通信中に起こる例外を表示します。
debug ip sla trace twamp connection	IP SLA TWAMP クライアントとサーバ間の正常な通信を表示します。
debug ip sla trace twamp control reflector	IP SLA TWAMP リフレクタによって送信された TWAMP サーバへの正常な通信を表示します。

debug ip sla trace twamp control server	IP SLA TWAMP サーバによって送信された TWAMP リフレクタへの正常な通信を表示します。
debug ip sla trace twamp session	IP SLA TWAMP 送信元とリフレクタ間の正常な通信を表示します。
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 ip sla error twamp session

Cisco IOS IP サービス レベル契約 (SLA) 双方向アクティブ測定プロトコル (TWAMP) のデバッグ出力をイネーブルにするには、**debug ip sla error twamp session** コマンドを特権 EXEC モードで使用します。このデバッグ出力は、TWAMP 送信元とリフレクタとの通信中に発生する例外を示します。デバッグ出力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 sla error twamp session [source-ip ip-address]

no debug ip sla error twamp session [source-ip ip-address]

構文の説明

source-ip ip-address (任意) 指定したソースの IP Performance Metrics (IPPM; IP パフォーマンスメトリック) TWAMP 接続をデバッグします。クライアントデバイスの IP アドレスを使用するソースを指定します。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

debug ip sla error twamp session 特権 EXEC コマンドは、TWAMP 送信元とリフレクタとの通信に関するエラー メッセージを表示します。



(注)

debug ip sla error twamp session コマンドではデバッグ出力が比較的少なく生成されるため、**debug ip sla trace twamp session** コマンドを使用する前に、**debug ip sla error twamp session** コマンドを使用します。

debug ip sla error twamp session コマンドは IPv4 ネットワークでサポートされます。

undebug ip sla error twamp session コマンドは、**no debug ip sla error twamp session** コマンドと同じです。

関連コマンド

コマンド	説明
debug ip sla error twamp connection	IP SLA TWAMP クライアントとサーバとの通信中に起こる例外を表示します。
debug ip sla error twamp control reflector	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp control server	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla trace twamp connection	IP SLA TWAMP クライアントとサーバ間の正常な通信を表示します。
debug ip sla trace twamp control reflector	IP SLA TWAMP リフレクタによって送信された TWAMP サーバへの正常な通信を表示します。

debug ip sla trace twamp control server	IP SLA TWAMP サーバによって送信された TWAMP リフレクタへの正常な通信を表示します。
debug ip sla trace twamp control server	IP SLA TWAMP 送信元とリフレクタ間の正常な通信を表示します。
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 ip sla trace twamp connection

Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) クライアントとサーバとの正常な通信を表示するには、**debug ip sla trace twamp connection** コマンドを特権 EXEC モードで使用します。デバッグ出力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 sla trace twamp connection [source-ip ip-address]

no debug ip sla trace twamp connection [source-ip ip-address]

構文の説明

source-ip ip-address (任意) 指定したソースの IP Performance Metrics (IPPM; IP パフォーマンスメトリック) TWAMP 接続をデバッグします。クライアント デバイスの IP アドレスを使用するソースを指定します。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

debug ip sla trace twamp connection 特権 EXEC コマンドでは、TWAMP セッション中のクライアントとサーバとの正常な通信に関するメッセージが表示されます。



(注)

debug ip sla error twamp connection コマンドではデバッグ出力が比較的少なく生成されるため、**debug ip sla trace twamp connection** コマンドを使用する前に、**debug ip sla error twamp connection** コマンドを使用します。

debug ip sla trace twamp connection コマンドは IPv4 ネットワークでサポートされます。

undebug ip sla trace twamp connection コマンドは、**no debug ip sla trace twamp connection** コマンドと同じです。

関連コマンド

コマンド	説明
debug ip sla error twamp connection	IP SLA TWAMP クライアントとサーバとの通信中に起こる例外を表示します。
debug ip sla error twamp control reflector	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp control server	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp session	IP SLA TWAMP 送信元とリフレクタとの通信中に起こる例外を表示します。
debug ip sla trace twamp control reflector	IP SLA TWAMP リフレクタによって送信された TWAMP サーバへの正常な通信を表示します。

debug ip sla trace twamp control server	IP SLA TWAMP サーバによって送信された TWAMP リフレクタへの正常な通信を表示します。
debug ip sla trace twamp session	IP SLA TWAMP 送信元とリフレクタ間の正常な通信を表示します。
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 ip sla trace twamp control reflector

TWAMP サーバとリフレクタとの間における Cisco IOS IP Service Level Agreement (SLA; サービスレベル契約) Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) の正常な通信のデバッグ出力をイネーブルにするには、**debug ip sla trace twamp control reflector** コマンドを特権 EXEC モードで使用します。デバッグ出力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 sla trace twamp control reflector

no debug ip sla trace twamp control reflector

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

debug ip sla trace twamp control reflector 特権 EXEC コマンドは、リフレクタからサーバに送信された通常の TWAMP セッションの通信に関するメッセージを表示します。



(注)

debug ip sla error twamp control reflector コマンドではデバッグ出力が比較的少なく生成されるため、**debug ip sla trace twamp control reflector** コマンドを使用する前に、**debug ip sla error twamp control reflector** コマンドを使用します。

debug ip sla trace twamp control reflector コマンドは IPv4 ネットワークでサポートされます。

undebug ip sla trace twamp control reflector コマンドは、**no debug ip sla trace twamp control reflector** コマンドと同じです。

関連コマンド

コマンド	説明
debug ip sla error twamp connection	IP SLA TWAMP クライアントとサーバとの通信中に起こる例外を表示します。
debug ip sla error twamp control reflector	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp control server	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp session	IP SLA TWAMP 送信元とリフレクタとの通信中に起こる例外を表示します。
debug ip sla trace twamp connection	IP SLA TWAMP クライアントとサーバ間の正常な通信を表示します。

debug ip sla trace twamp control server	IP SLA TWAMP サーバによって送信された TWAMP リフレクタへの正常な通信を表示します。
debug ip sla trace twamp session	IP SLA TWAMP 送信元とリフレクタ間の正常な通信を表示します。
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 ip sla trace twamp control server

TWAMP サーバとリフレクタとの間における Cisco IOS IP Service Level Agreement (SLA; サービスレベル契約) Two-Way Active Measurement Protocol (TWAMP; 双方向アクティブ測定プロトコル) の正常な通信のデバッグ出力をイネーブルにするには、**debug ip sla trace twamp control server** コマンドを特権 EXEC モードで使用します。デバッグ出力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 sla trace twamp control server

no debug ip sla trace twamp control server

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

debug ip sla trace twamp control server 特権 EXEC コマンドは、サーバからリフレクタに送信された通常の TWAMP セッションの通信に関するメッセージを表示します。



(注)

debug ip sla error twamp control server コマンドではデバッグ出力が比較的少なく生成されるため、**debug ip sla trace twamp control server** コマンドを使用する前に、**debug ip sla error twamp control server** コマンドを使用します。

debug ip sla trace twamp control server コマンドは IPv4 ネットワークでサポートされます。

undebug ip sla trace twamp control server コマンドは、**no debug ip sla trace twamp control server** コマンドと同じです。

関連コマンド

コマンド	説明
debug ip sla error twamp connection	IP SLA TWAMP クライアントとサーバとの通信中に起こる例外を表示します。
debug ip sla error twamp control reflector	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp control server	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp session	IP SLA TWAMP 送信元とリフレクタとの通信中に起こる例外を表示します。
debug ip sla trace twamp connection	IP SLA TWAMP クライアントとサーバ間の正常な通信を表示します。

debug ip sla trace twamp control reflector	IP SLA TWAMP リフレクタによって送信された TWAMP サーバへの正常な通信を表示します。
debug ip sla trace twamp session	IP SLA TWAMP 送信元とリフレクタ間の正常な通信を表示します。
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 ip sla trace twamp session

TWAMP 送信元とリフレクタとの間における Cisco IOS IP サービス レベル契約 (SLA) 双方向アクティブ測定プロトコル (TWAMP) の通常のセッション通信のデバッグ出力をイネーブルにするには、**debug ip sla trace twamp session** コマンドを特権 EXEC モードで使用します。デバッグ出力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 sla trace twamp session [**source-ip** *ip-address* | **source-port** *port-number*]

no debug ip sla trace twamp session [**source-ip** *ip-address* | **source-port** *port-number*]

構文の説明

source-ip *ip-address* (任意) 指定したソースの IP Performance Metrics (IPPM; IP パフォーマンスメトリック) TWAMP 接続をデバッグします。クライアント デバイスの IP アドレスを使用するソースを指定します。

source-port *port-number* (任意) 指定したポートの IP パフォーマンス メトリック (IPPM) TWAMP 接続をデバッグします。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

debug ip sla trace twamp session 特権 EXEC コマンドは、TWAMP 送信元とリフレクタとの通常のセッション通信を表示します。



(注)

debug ip sla error twamp session コマンドではデバッグ出力が比較的少なく生成されるため、**debug ip sla trace twamp session** コマンドを使用する前に、**debug ip sla error twamp session** コマンドを使用します。

debug ip sla trace twamp session コマンドは IPv4 ネットワークでサポートされます。

undebug ip sla trace twamp session コマンドは、**no debug ip sla trace twamp session** コマンドと同じです。

関連コマンド

コマンド	説明
debug ip sla error twamp connection	IP SLA TWAMP クライアントとサーバとの通信中に起こる例外を表示します。
debug ip sla error twamp control reflector	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp control server	IP SLA TWAMP サーバとリフレクタとの通信中に起こる例外を表示します。
debug ip sla error twamp session	IP SLA TWAMP 送信元とリフレクタとの通信中に起こる例外を表示します。

debug ip sla trace twamp connection	IP SLA TWAMP クライアントとサーバ間の正常な通信を表示します。
debug ip sla trace twamp control reflector	IP SLA TWAMP リフレクタによって送信された TWAMP サーバへの正常な通信を表示します。
debug ip sla trace twamp control server	IP SLA TWAMP サーバによって送信された TWAMP リフレクタへの正常な通信を表示します。
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 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	変更箇所
12.2(53)EX	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。

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 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]



(注) LACP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

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	変更箇所
12.2(53)EX	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。

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 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	変更箇所
12.2(53)EX	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。

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	変更箇所
12.2(53)EX	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。

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	変更箇所
12.2(53)EX	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。

関連コマンド

コマンド	説明
mac address-table move update	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; 簡易ネットワーク管理プロトコル) 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	変更箇所
12.2(53)EX	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。

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	変更箇所
12.2(53)EX	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。

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 nvram

NVRAM 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	変更箇所
12.2(53)EX	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。

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** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **event** | **fsm** | **misc** | **packet**]



(注) PAgP を使用できるのは、ネットワーク ノード インターフェイス (NNI) および拡張ネットワーク インターフェイス (ENI) 上だけです。

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。
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	変更箇所
12.2(53)EX	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 pagp コマンドは、**no debug pagp** コマンドと同じです。

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 | vacl | vlmmap | warn}
```

```
no debug platform acl {all | exit | label | main | vacl | vlmmap | 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。
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。



(注)

stack キーワードは、コマンドラインのヘルプ スtring には表示されていますが、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	変更箇所
12.2(53)EX	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。

関連コマンド

コマンド	説明
show debugging	イネーブ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 cfm

イーサネット接続障害管理 (CFM) サービスのデバッグをイネーブルにするには、**debug platform cfm** 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 cfm

no debug platform cfm

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

CFM は、サービス インスタンス単位のエンドツーエンド イーサネット レイヤ運用管理および保守 (OAM) プロトコルです。大規模イーサネット ネットワークに接続モニタリング、障害検証、および障害隔離を提供します。

undebug platform cfm コマンドは、**no debug platform cfm** コマンドと同じです。

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。

コマンド 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform backup interface コマンドは、**no platform debug backup interface** コマンドと同じです。

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; リバース パス転送) 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	変更箇所
12.2(53)EX	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。

関連コマンド

コマンド	説明
<code>show debugging</code>	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

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 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; リモート プロシージャ コール) 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	変更箇所
12.2(53)EX	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。

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-detailed | rpc-generic | warnings}

no debug platform etherchannel {init | link-up | rpc-detailed | rpc-generic | 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-detailed	EtherChannel Remote Procedure Call (RPC; リモート プロシージャ コール) の詳細なデバッグ メッセージを表示します。
rpc-generic	EtherChannel RPC の一般的なデバッグ 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	変更箇所
12.2(53)EX	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。

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 Content Addressable Memory (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	変更箇所
12.2(53)EX	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。

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 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; リモート プロシージャ コール) 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform ip arp inspection コマンドは、**no debug platform ip arp inspection** コマンドと同じです。

関連コマンド

コマンド	説明
show ip arp inspection	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; リモートプロシージャコール) 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	変更箇所
12.2(53)EX	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。

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 | 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; リモート プロシージャ コール) 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 { <i>ip-address</i> error ipopt leave query report rx svi tx }	<p>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。</p> <ul style="list-style-type: none"> 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; スイッチ仮想インターフェイス) 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。
private-vlan	IGMP スヌーピング プライベート VLAN 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。

■ debug platform ip igmp snooping

rpc [cfg l3mm misc vlan]	IGMP スヌーピング Remote Procedure Call (RPC; リモート プロシージャ コール) 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。 <ul style="list-style-type: none"> • 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	変更箇所
	12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン `undebg platform ip igmp snooping` コマンドは、`no debug platform ip igmp snooping` コマンドと同じです。

関連コマンド	コマンド	説明
	<code>debug ip igmp snooping</code>	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。
	<code>show debugging</code>	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 {acl-full-events | 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 {acl-full-events | 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

acl-full-events	IP-multicast 出力 ACL の完全なデバッグ 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 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 Rendezvous 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; リバース パス転送) 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

■ debug platform ip multicast

コマンド履歴	リリース	変更箇所
	12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン `undebg platform ip multicast` コマンドは、`no debug platform ip multicast` コマンドと同じです。

関連コマンド	コマンド	説明
	<code>show debugging</code>	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	変更箇所
12.2(53)EX	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 Content Addressable Memory (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; リモート プロシージャ コール) 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; ホットスタンバイ ルータ プロトコル) 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。
table	IP ユニキャスト ルーティング IPv4 テーブル デバッグ メッセージを表示します。
vrf	IP ユニキャスト ルーティング VRF 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	変更箇所
	12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン `undebg platform ip unicast` コマンドは、`no debug platform ip unicast` コマンドと同じです。

関連コマンド	コマンド	説明
	<code>show debugging</code>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform ipc コマンドは、**no debug platform ipc** コマンドと同じです。

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}
```

```
no debug platform led {generic | signal}
```

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。



(注)

stack 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。

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	変更箇所
12.2(53)EX	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。

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 ラーニング 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; リモート プロシージャ コール) 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 ラーニング 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform matm コマンドは、**no debug platform matm** コマンドと同じです。

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 | usererr}
```

```
no debug platform messaging application {all | badpak | cleanup | events | memerr |
  messages | 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。
usererr	ユーザ エラー デバッグ メッセージを表示します。



(注)

stackchg 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。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform messaging application コマンドは、**no debug platform messaging application** コマンドと同じです。

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 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}
```

```
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}
```

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	デュアルパーパス PHY イベントを表示します。
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。 <ul style="list-style-type: none"> • configure : PHY 設定デバッグ メッセージを表示します。 • ipc : プロセス間通信 (IPC) 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 小型フォーム ファクタ (SFP) 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。



(注)

xenpak キーワードは、コマンドラインのヘルプ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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

`undebg platform phy` コマンドは、`no debug platform phy` コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	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 | errrdisable | etherchnl | exceptions | hpm-events |
idb-events | if-numbers | ios-events | link-status | platform | pm-events | pm-vectors
[detail] | rpc [general | oper-info | state | vectors | vp-events] | soutput | sync | vlans}
```

```
no debug platform pm {all | counters | errrdisable | etherchnl | exceptions | hpm-events |
idb-events | if-numbers | ios-events | link-status | platform | pm-events | pm-vectors
[detail] | rpc [general | oper-info | state | vectors | vp-events] | soutput | 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; リモートプロシージャコール) デバッグメッセージのカウンタを表示します。
errrdisable	errrdisable 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	IOS イベントの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-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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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	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。
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。



(注) **stack-manager** キーワードは、コマンドラインのヘルプ スtring には表示されていますが、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

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン **undebg platform pm** コマンドは、**no debug platform pm** コマンドと同じです。

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 policer cpu uni-eni

ユーザ ネットワーク インターフェイス (UNI) および拡張ネットワーク インターフェイス (ENI) でコントロールプレーンポリサーのデバッグをイネーブルにするには、**debug platform policer cpu uni-eni** 特権 EXEC コマンドを使用します。このコマンドにより、CPU 保護に対して何らかの変更があった場合に、情報メッセージが表示されます。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 policer cpu uni-eni

no debug platform policer cpu uni-eni

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebbug platform policer cpu uni-eni コマンドは、**no debug platform policer cpu uni-eni** コマンドと同じです。

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 policer cpu	機能、インデックス、および特定のポートの対応する機能ごとに、コントロールプレーンポリサーの統計情報を表示します。

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 | write}

no debug platform port-asic {interrupt | periodic | read | 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。
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	変更箇所
12.2(53)EX	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。

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; リモート プロシージャ コール) 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	変更箇所
12.2(53)EX	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。

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 Content Addressable Memory (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 | ms-entry | ms-mask |
rpc | tcam}
```

```
no debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | ms-entry | ms-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。
ms-entry	QATM MS エントリ関連イベント デバッグ メッセージを表示します。
ms-mask	QATM MS 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; リモート プロシージャ コール) 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	変更箇所
12.2(53)EX	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。

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-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 platform 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 platform qos-manager {all | event | verbose}
```

```
no debug platform qos-manager {all | event | verbose}
```

構文の説明

all	QoS マネージャ デバッグ メッセージをすべて表示します。
event	QoS マネージャ イベント デバッグ メッセージを表示します。
verbose	詳細 QoS 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

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform qos-manager コマンドは、**no debug platform qos-manager** コマンドと同じです。

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	変更箇所
12.2(53)EX	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。

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 rep

Resilient Ethernet Protocol (REP) のデバッグをイネーブルにするには、**debug platform rep** 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 rep

no debug platform rep

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	変更箇所
12.2(53)EX	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 rep コマンドは、**no debug platform rep** コマンドと同じです。

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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform resource-manager コマンドは、**no debug platform resource-manager** コマンドと同じです。

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; 簡易ネットワーク管理プロトコル) 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	変更箇所
12.2(53)EX	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。

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; スイッチド ポート アナライザ) 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	変更箇所
12.2(53)EX	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。

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。
jumbo	スーパーバイザ ASIC ジャンボ 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform supervisor-asic コマンドは、**no debug platform supervisor-asic** コマンドと同じです。

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	変更箇所
12.2(53)EX	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。

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 Content Addressable Memory (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} | 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} | 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。 <ul style="list-style-type: none"> • 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} 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。 <ul style="list-style-type: none"> • 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。 • 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。 <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>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。</p> <p>tcam : TCAM 書き込みデバッグ メッセージを表示します。</p>



(注)

log l3 ipv6 {acl {input | output} | local | qos | secondary} 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform tcam コマンドは、**no debug platform tcam** コマンドと同じです。

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 uddld

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 uddld** 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 uddld [**all** | **error** | **rpc** {**events** | **messages**}]

no debug platform uddld [**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; リモートプロシージャコール) 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。 <ul style="list-style-type: none"> 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg platform uddld コマンドは、**no debug platform uddld** コマンドと同じです。

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; リモート プロシージャ コール) 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	変更箇所
12.2(53)EX	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。

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 | cookies | etherchnl | hatable | messages | port | registry |
sm | span | split | vlan | vp}
```

```
no debug pm {all | assert | card | cookies | etherchnl | hatable | messages | port | 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。
cookies	内部 PM クッキー検証デバッグ 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。
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tring 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	変更箇所
12.2(53)EX	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 pm コマンドは、**no debug pm** コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	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タス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	変更箇所
12.2(53)EX	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。

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	変更箇所
12.2(53)EX	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。

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 scada modbus tcp server

Modicon Communication Bus (MODBUS) TCP ソフトウェアのデバッグをイネーブルにするには、**debug scada modbus tcp server** 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 scada modbus tcp server {errors | events | verbose}
```

```
no debug scada modbus tcp server {errors | events | verbose}
```

構文の説明

errors	すべての MODBUS TCP サーバ エラーを表示します。
events	MODBUS TCP サーバ関連イベント デバッグ メッセージを表示します。
verbose	MODBUS TCP サーバの詳細なデバッグ 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	変更箇所
12.2(53)EX	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 scada modbus tcp server コマンドは、**no debug scada modbus tcp server** コマンドと同じです。

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 | bpdu | bpdu-opt | config | etherchannel | events | exceptions |
                    general | mstp | pvst+ | root | snmp | switch | synchronization}
```

```
no debug spanning-tree {all | bpdu | bpdu-opt | config | etherchannel | events | exceptions
                       | general | mstp | pvst+ | root | snmp | switch | synchronization}
```

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。
bpdu	スパニング ツリー Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) デバッグ メッセージを表示します。 debug spanning-tree bpdu コマンドを参照してください。
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。 debug spanning-tree bpdu-opt コマンドを参照してください
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。
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。 debug spanning-tree mstp コマンドを参照してください
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; 簡易ネットワーク管理プロトコル) 処理デバッグ 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; スパニング ツリー プロトコル) 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。 debug spanning-tree switch コマンドを参照してください
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。



(注)

backbonefast、**csuf/csrt**、および **uplinkfast** キーワードは、コマンドラインのヘルプ スtring 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。

■ debug spanning-tree

コマンドモード 特権 EXEC

コマンド履歴	リリース	変更箇所
	12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン undebg spanning-tree コマンドは、no debug spanning-tree コマンドと同じです。

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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg spanning-tree bpdu コマンドは、**no debug spanning-tree bpdu** コマンドと同じです。

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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg spanning-tree bpdu-opt コマンドは、**no debug spanning-tree bpdu-opt** コマンドと同じです。

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。 <ul style="list-style-type: none"> Multiple Spanning-Tree (MST) リージョンと、Rapid Spanning-Tree Protocol (RSTP; 高速スパニング ツリー プロトコル) 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、IEEE 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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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

■ debug spanning-tree mstp

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

`undebg spanning-tree mstp` コマンドは、`no debug spanning-tree mstp` コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	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。
<code>show spanning-tree</code>	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; スパニング ツリー プロトコル) 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]}
```

```
no debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors | interrupt | process} | state | tx [decode]}
```

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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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。 <ul style="list-style-type: none"> • 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; 割り込みサービス要求) 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。 <ul style="list-style-type: none"> • decode : (任意) デコードされた送信パケットを表示します。



(注)

uplinkfast 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

■ debug spanning-tree switch

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

`undebg spanning-tree switch` コマンドは、`no debug spanning-tree switch` コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	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。
<code>show spanning-tree</code>	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 |
notification | packets | registries}
```

```
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management |
notification | packets | registries}
```

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。 <ul style="list-style-type: none"> 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; コマンドライン インターフェイス) 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。
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。
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。

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	変更箇所
12.2(53)EX	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。

■ debug sw-vlan

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 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。 <ul style="list-style-type: none"> 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg sw-vlan ifs コマンドは、**no debug sw-vlan ifs** コマンドと同じです。

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

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 | allowedvlanfcgchange | fwdchange |
linkchange | modechange | statechange}
```

```
no debug sw-vlan notification {accfwdchange | allowedvlanfcgchange | fwdchange |
linkchange | modechange | 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。
allowedvlanfcgchange	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。
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。



(注) **pruningfcgchange** 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	変更箇所
12.2(53)EX	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。

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 udld

Unidirectional Link Detection (UDLD; 単方向リンク検出) 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ッチャ 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

undebg udld コマンドは、**no debug udld** コマンドと同じです。

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 uddl 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 uddl	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 ラーニング 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	変更箇所
12.2(53)EX	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。

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。



APPENDIX A

Cisco CGS 2520 スイッチのブート ロードー コマンド

この付録では、Cisco CGS 2520 スイッチのブートローダー コマンドについて説明します。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、電源投入時自己診断テスト (POST) 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て、接続し直します。スイッチは POST の実行後、自動起動プロセスを開始します。ブートローダは、ブートアップ シーケンス中にユーザにブレイク キーの文字を求めるプロンプトを表示します (次の例を参照)。

```
***** The system will autoboot in 15 seconds *****
```

```
Send a break key to prevent autobooting.
```

ブレイク キーの文字は、オペレーティング システムごとに異なります。

- UNIX を実行している SUN ワークステーションでは、Ctrl+C がブレイク キーです。
- Windows 2000 を実行する PC では、Ctrl+Break がブレイク キーとなります。

Cisco TAC では、一般的なオペレーティング システムのブレイク キー、およびブレイク キーをサポートしていない端末エミュレータで使用できる代替ブレイク キー シーケンスに関するリストが用意されています。このリストを参照する場合は、次の URL にアクセスしてください。

<http://www.cisco.com/warp/public/701/61.html#how-to>

ブレイク キーを入力すると、ブートローダの 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ブートして、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。
<i>filesystem</i>:	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。
<i>/file-url</i>	(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ブートしようとします。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	変更箇所
12.2(53)EX	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ブートしようとします。**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ブートしようとします。

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ブート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ブート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。

■ boot

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

<i>filesystem:</i>	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。
<i>/file-url</i>	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	変更箇所
12.2(53)EX	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: cat flash:/new-images/info flash:env_vars
version_suffix: image-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: me340x
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 <i>block-size</i>	(任意) このオプションは、内部開発およびテスト専用です。
<i>filesystem:</i>	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。
<i>/source-file-url</i>	コピー元のパス (ディレクトリ) およびファイル名です。
<i>/destination-file-url</i>	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	変更箇所
12.2(53)EX	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	
<i>filesystem:</i>	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。
<i>/file-url</i>	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	変更箇所
	12.2(53)EX	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

<i>filesystem:</i>	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。
<i>/file-url</i>	(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	変更箇所
12.2(53)EX	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  image-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) <ul style="list-style-type: none">• 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	変更箇所
12.2(53)EX	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、通常のブート 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	変更箇所
12.2(53)EX	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 ロードー 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 ロードー

コマンド履歴

リリース	変更箇所
12.2(53)EX	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	変更箇所
12.2(53)EX	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	変更箇所
12.2(53)EX	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)
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。
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	
<i>filesystem:</i>	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。
<i>/directory-url</i>	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	変更箇所
	12.2(53)EX	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示します。

```
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 ロードー コマンドを使用します。

more *filesystem:/file-url ...*

構文の説明

<i>filesystem:</i>	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。
<i>/file-url</i>	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 ロードー

コマンド履歴

リリース	変更箇所
12.2(53)EX	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-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: 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

<i>filesystem:</i>	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。
<i>/source-file-url</i>	元のパス (ディレクトリ) およびファイル名です。
<i>/destination-file-url</i>	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	変更箇所
12.2(53)EX	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	変更箇所
12.2(53)EX	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ブートして、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	<i>filesystem:</i>	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。
	<i>/directory-url</i>	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	変更箇所
	12.2(53)EX	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。

sd_init

内部 Secure Digital (SD) フラッシュ メモリ カードを再初期化するには、**sd_init** ブート ローダー コマンドを使用します。

sd_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。

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

通常の運用では、SD フラッシュ メモリ カードはカバーの後ろに安全に装着されたままになっています。**sd_init** コマンドは、スイッチをリセットした後、またはスイッチがブート ローダー モードで実行されていたときに SD フラッシュ メモリ カードを取り外して再装着した後にのみ使用します。

PC など他のタイプのデバイスで CGS 2520 SD フラッシュ メモリ カードを使用しないでください。SD フラッシュ メモリ カードのデータの形式は、一般的な SD フラッシュ メモリ カードと互換性がありません。

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



(注) 通常的环境では、環境変数の設定を変更する必要はありません。

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 : スイッチを自動でブートするか、または手動でブート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、ブートローダはシステムを自動的に起動しようとします。他の値に設定されている場合は、ブートローダ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 : 自動ブート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 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かった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。

ENABLE_BREAK : コンソール上のブレイク キーを使用して自動ブート 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ブレイク キーを押して、自動ブート 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) (コンソール上でブレイク キーを押して自動ブート 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	変更箇所
12.2(53)EX	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。

通常的环境では、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。

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。

ブート ローダーのプロンプト スtring (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

<i>filesystem:</i>	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。
<i>/file-url</i>	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	変更箇所
12.2(53)EX	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-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: 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 ...



(注) 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。

構文の説明

<i>variable</i>	<p><i>variable</i> には、次に示すキーワードのいずれかを使用します。</p> <p>MANUAL_BOOT : スイッチを自動でブートするか、または手動でブートするかを決定します。</p> <p>BOOT : 自動ブート時に、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 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かった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。</p> <p>ENABLE_BREAK : フラッシュ ファイル システムの初期化後に、コンソール上のブレイク キーを使用して自動ブート プロセスを中断できるかどうかを決定します。</p> <p>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。</p> <p>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</p> <p>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。</p> <p>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。</p> <p>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。</p>
-----------------	--

コマンド モード

ブート ローダー

コマンド履歴

リリース	変更箇所
12.2(53)EX	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。

例

次の例では、プロンプト スtring 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	変更箇所
12.2(53)EX	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  
switch-name Boot Loader (xxxxxx-HBOOT-M) Version 12.2(xx)EX  
Compiled Wed 12-Sept-05 14:58 by devgoyal
```

```
switch:
```

■ version



APPENDIX **B**

Cisco CGS 2520 の Show Platform コマンド

この付録では、Cisco CGS 2520 スイッチで使用するため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。 <i>label-number</i> 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。 <ul style="list-style-type: none"> 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 統計情報を表示します。 <i>asic-number</i> は、常に 0 のポート ASIC 番号です。
usage asic-number [summary]	ASIC 単位の ACL 使用状況を表示します。 <i>asic-number</i> は、常に 0 のポート ASIC 番号です。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> summary : (任意) 簡単な使用状況情報を表示します。
vlan vlan-id	VLAN 単位の ACL マネージャ情報を表示します。 <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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

<i>interface-id</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 cfm

プラットフォームに依存するイーサネット接続障害管理 (CFM) 情報を表示するために **show platform cfm** 特権 EXEC コマンドを使用します。CFM は、エンドツーエンドのサービス インスタンス単位のイーサネット レイヤ Operation, Administration, and Management (OAM) プロトコルで、大規模イーサネット ネットワークに事前接続モニタリング、障害検証、および障害隔離を提供します。

```
show platform cfm [ | {begin | exclude | include} expression]
```

構文の説明

コマンド モード 特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(53)EX	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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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作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 dl

動的にロードされるモジュールの情報を表示するには、**show platform dl** 特権 EXEC コマンドを使用します。

```
show platform dl [detail] [| {begin | exclude | include} expression]
```

構文の説明

detail	(任意) 動的にロードされるモジュールの詳細情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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] [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 | tcp src-port dst-port flags | udp src-port dst-port} [ | {begin | exclude | include} expression]
```

構文の説明

<i>interface-id</i>	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 (タイプ、ポート番号を含む)。
vlan <i>vlan-id</i>	(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。
<i>src-mac</i>	48 ビット送信元 MAC アドレス。
<i>dst-mac</i>	48 ビット宛先 MAC アドレス。
<i>l3protocol-id</i>	(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。
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 <i>cos</i>	(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 <i>src-ip</i> <i>dst-ip</i>	(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 <i>field</i>	(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 <i>dscp</i>	(任意) IP ヘッダーの Differentiated Service Code Point (DSCP; DiffServ コード ポイント) フィールド。指定できる範囲は 0 ~ 63 です。
<i>l4protocol-id</i>	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、UDP、ICMP、または IGMP の場合、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 <i>icmp-type</i> <i>icmp-code</i>	インターネット制御メッセージプロトコル (ICMP) パラメータ。 <i>icmp-type</i> および <i>icmp-code</i> に指定できる範囲は 0 ~ 255 です。
igmp <i>igmp-version</i> <i>igmp-type</i>	Internet Group Management Protocol (IGMP; インターネット グループ 管理プロトコル) のパラメータ。指定できる範囲は、 <i>igmp-version</i> は 1 ~ 15、 <i>igmp-type</i> は 0 ~ 15 です。
tcp <i>src-port</i> <i>dst-port</i> <i>flags</i>	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。 <i>src-port</i> および <i>dst-port</i> 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 <i>src-port dst-port</i>	User Datagram Protocol (UDP; ユーザ データグラム プロトコル) のパラメータ。 <i>src-port</i> および <i>dst-port</i> に指定できる範囲は 0 ~ 65535 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の文字列です。



(注) **ipv6** キーワードは、コマンドラインのヘルプ スtring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	変更箇所
12.2(53)EX	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

show platform forward のコマンド出力の表示の例およびその意味については、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]
```

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	<i>number</i> 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。 <i>number</i> 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	<i>number</i> 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。 <i>number</i> 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	<i>number</i> 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。指定できる範囲は 0 ~ 1 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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、 <i>ip-address</i> 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> count : (任意) リモート カウントだけを表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	このコマンドが追加されました。

■ show platform ip igmp snooping

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 | retry | 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。
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。
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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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

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 | route | standby | statistics | 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 データベースの現在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。 <ul style="list-style-type: none"> • 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 : ハードウェアでのプログラミングに失敗したルート 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。
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。
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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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。

```
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]
```



(注) このコマンドは、スイッチでメトロ IP アクセスイメージが稼動しており、スイッチにデュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを設定している場合にだけ使用できます。

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。
<i>ipv6-prefix</i>	(任意) 表示する IPv6 ネットワーク。このアドレスは、16 ビット値をコロンで区切った 16 進数で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。 <ul style="list-style-type: none"> 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 <i>ipv6-prefix/prefix length</i>	IPv6 プレフィクス圧縮情報を表示します。 <ul style="list-style-type: none"> <i>ipv6-prefix</i> : IPv6 ネットワークです。 <i>/prefix length</i> : 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。 <ul style="list-style-type: none"> 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 ハードウェア 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の文字列です。

■ show platform ipv6 unicast

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更箇所
	12.2(53)EX	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 l2pt dm

レイヤ 2 プロトコル トンネリング宛先マップおよび関連付けられたポートを表示するには **show platform l2pt dm** 特権 EXEC コマンドを使用します。

```
show platform l2pt dm [ | {begin | exclude | include} expression]
```

構文の説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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 | 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。
qos [<i>port-asic</i>]	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。 <ul style="list-style-type: none"> <i>port-asic</i> : (任意) QoS ポート ASIC 番号。値は 0 または 1 を指定できます。
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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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、 <i>mac-address</i> 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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	変更箇所
12.2(53)EX	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] | hipperf
[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。 <ul style="list-style-type: none"> • 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。
hipperf [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、 <i>class-number</i> 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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 <i>session-number</i>	(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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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 | 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。 <ul style="list-style-type: none"> 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。
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。 <ul style="list-style-type: none"> 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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) **stack-view** 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	変更箇所
12.2(53)EX	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 policer cpu

機能ごとの CPU コントロール プレーン ポリサーの統計情報、または指定されたポートのインデックスと対応する機能を表示するには、**show platform policer cpu** 特権 EXEC コマンドを使用します。

```
show platform policer cpu {classification | interface interface-id} [| {begin | exclude | include} expression]
```

構文の説明

classification	機能ごとのポリサー統計情報を表示します。
interface <i>interface-id</i>	特定のインターフェイスのポリサー インデックスを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	このコマンドが追加されました。

使用上のガイドライン

ユーザ ネットワーク インターフェイス (UNI) および拡張ネットワーク インターフェイス (ENI) の CPU 保護のために、スイッチは 0 ~ 26 の番号の付けられた 27 個の CPU 保護ポリサーを事前に割り当てます。ポリサー 26 は、廃棄ポリサーを意味しています。いずれのポートでも、26 として示されるすべてのトラフィック タイプはドロップされます。ポリサー 0 ~ 25 はレート制限ポリサーで、制御プロトコルのポートに割り当てられます。ポリサー 255 は、ポリサーが制御プロトコルに割り当てられないことを意味します。ネットワーク ノード インターフェイス (NNI) にはポリサーが割り当てられていません。

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。

show platform policer cpu

例

これは **show platform policer cpu classification** コマンドの出力例を示します。

```
Switch# show platform policer cpu classification
=====
SWITCH 1
=====
Feature                               Bytes           Frames
=====
STP                                    3912792         61278
LACP                                    0               0
8021X                                   0               0
RSVD_STP                               0               0
PVST_PLUS                              0               0
CDP                                     1012542         2552
DTP                                     131264          2051
UDLD                                    0               0
PAGP                                    0               0
VTP                                     0               0
CISCO_L2                               0               0
KEEPALIVE                              0               0
CFM                                     0               0
SWITCH_MAC                             0               0
SWITCH_ROUTER_MAC                      896             14
SWITCH_IGMP                             289408          4522
SWITCH_L2PT                             0               0
```

次の **show platform policer cpu interface** コマンドの出力例は、UNI のデフォルトのポリサーの設定を示します。ポートがファストイーサネット 1 であるため、レート制限されるプロトコルの ID は 0 で、ファストイーサネットポート 5 には、ID 4 が表示されます。*Policer Index* は、特定のプロトコルを意味します。ASIC 番号は、ポリサーが異なる ASIC 上にある場合を表します。

UNI では、STP、CDP、LLDP、LACP、および PAgP がサポートされていないので、これらのパケットは破棄されます（物理ポリサー 26）。ENI でもこれらのプロトコルはデフォルトでディセーブルになっていますが、イネーブルにすることが可能です。ENI 上でイネーブルにすると、制御パケットがレート制限され、レート制限ポリサーが、これらのプロトコルのポートに割り当てられます（物理ポリサー 22）。

```
Switch# show platform policer cpu interface fastethernet 0/3
Policers assigned for CPU protection
=====
Feature                               Policer         Physical       Asic
Index                                 Policer         Num
=====
Fa0/1
STP                                    1               26             0
LACP                                    2               26             0
8021X                                   3               26             0
RSVD_STP                               4               26             0
PVST_PLUS                              5               26             0
CDP                                     6               26             0
LLDP                                    7               26             0
DTP                                     8               26             0
UDLD                                    9               26             0
PAGP                                    10              26             0
VTP                                    11              26             0
CISCO_L2                               12              26             0
KEEPALIVE                              13              0              0
CFM                                     14              255            0
SWITCH_MAC                             15              26             0
SWITCH_ROUTER_MAC                      16              26             0
SWITCH_IGMP                             17              0              0
SWITCH_L2PT                             18              26             0
```

次に、制御プロトコルがインターフェイス上でイネーブルになったときに ENI に割り当てられるポリサーの例を示します。値 22 は、プロトコル パケットが、そのプロトコルに関してレート制限されていることを示しています。プロトコルがイネーブルになっていない場合、デフォルトは UNI の場合と同じです。

```
Switch# show platform policer cpu interface fastethernet0/23
Policers assigned for CPU protection
=====
Feature                               Policer      Physical     Asic
Index                                  Policer      Num
=====
Fa0/23
STP                                    1            26           0
LACP                                    2            22           0
8021X                                   3            26           0
RSVD_STP                                4            26           0
PVST_PLUS                               5            26           0
CDP                                      6            22           0
LLDP                                    7            26           0
DTP                                      8            26           0
UDLD                                    9            26           0
PAGP                                    10           26           0
VTP                                     11           26           0
CISCO_L2                               12           22           0
KEEPALIVE                              13           22           0
CFM                                     14           255          0
SWITCH_MAC                             15           26           0
SWITCH_ROUTER_MAC                      16           26           0
SWITCH_IGMP                             17           22           0
SWITCH_L2PT                             18           22           0
```

次に、NNI に割り当てられるデフォルト ポリサーを示します。ほとんどのプロトコルでは、NNI にポリサーが割り当てられません。値 255 は、プロトコルのポートにポリサーが割り当てられないことを意味します。

```
Switch #show platform policer cpu interface gigabitethernet 0/1
Policers assigned for CPU protection
=====
Feature                               Policer      Physical     Asic
Index                                  Policer      Num
=====
Gi0/1
STP                                    1            255          0
LACP                                    2            255          0
8021X                                   3            255          0
RSVD_STP                                4            255          0
PVST_PLUS                               5            255          0
CDP                                      6            255          0
LLDP                                    7            255          0
DTP                                      8            255          0
UDLD                                    9            255          0
PAGP                                    10           255          0
VTP                                     11           255          0
CISCO_L2                               12           255          0
KEEPALIVE                              13           255          0
CFM                                     14           255          0
SWITCH_MAC                             15           255          0
SWITCH_ROUTER_MAC                      16           255          0
SWITCH_IGMP                             17           255          0
SWITCH_L2PT                             18           255          0
```

■ show platform policer cpu

関連コマンド	コマンド	説明
	show policer cpu uni-eni	スイッチのコントロールプレーン ポリサー情報を表示します。

show platform port-asic

プラットフォーム依存型ポート Application-Specific Integrated Circuit (ASIC; 特定用途向け集積回路) 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]
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]]}
[ | {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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 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 [<i>asic number</i> port number [<i>asic number</i>]]	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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 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 [<i>asic number</i> port number [<i>asic number</i>]]	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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 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 [<i>asic number</i> port number [<i>asic number</i>]]	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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 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 [<i>asic number</i>]	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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 です。
packet-info-ram [<i>asic number</i> index number [<i>asic number</i>]]	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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 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 [<i>asic number</i> port number [<i>asic number</i>]]	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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 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 [<i>asic number</i> port number [<i>asic number</i>]]	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。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。この番号は、常に 0 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]]	<p>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。</p> <ul style="list-style-type: none"> • 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。この番号は、常に 0 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]	<p>Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 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。</p> <ul style="list-style-type: none"> • 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。この番号は、常に 0 です。
stats { drop enqueue miscellaneous supervisor } [asic number port number [asic number]]	<p>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。</p> <ul style="list-style-type: none"> • 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。この番号は、常に 0 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]]	<p>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。</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の文字列です。



(注)

stack {**control** | **dest-map** | **learning** | **messages** | **mvid** | **prog-parser** | **span** | **stats** [**asic number** | **port number** [**asic number**]] 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	変更箇所
12.2(53)EX	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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
	12.2(53)EX	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 debug [aggregate-policer aggregate-policer-name | global-config |
input-queue | [interface [interface-id] [buffers | policers | queuing]] | label-table
[dynamic-label {dscp value cos value | label-number value | policy-map
policy-map-name class-map class-map-name} [asic number] | policer
{parameter-table | qos-table| selection-table} [asic number] | policy-map
policy-map-name [asic number] | port-class [asic number] | port-config port-number
[asic number] | port-info port-number [asic number] | table-map | vlan vlan-id] [ |
{begin | exclude | include} expression]
```

```
show platform qos statistics [interface [interface-id]] [ | {begin | exclude | include}
expression]
```

構文の説明

debug	スイッチまたは特定のキーワードの QoS デバッグ メッセージを表示します。
aggregate-policer <i>aggregate-policer-name</i>	(任意) 指定された集約ポリサーの QoS 集約ポリサー情報を表示します。
global-config	(任意) QoS のグローバル設定情報を表示します。
input-queue	(任意) QoS の入力キューの情報を表示します。
interface [<i>interface-id</i>] [buffers policers queuing]	(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 QoS 情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • buffers : (任意) QoS バッファに関する情報を表示します。 • policers : (任意) QoS ポリサーに関する情報を表示します。 • queuing : (任意) QoS の出力キューに関する情報を表示します。
label-table [dynamic-label { <i>dscp value cos value</i> label-number <i>value</i> policy-map <i>policy-map-name class-map class-map-name</i> } [asic number]	(任意) QoS ラベル 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。 <ul style="list-style-type: none"> • dynamic-label : (任意) ダイナミック ラベル情報を表示します。 • dscp value cos value : DiffServ コード ポイント (DSCP) 値 (0 ~ 63)、およびサービス クラス (CoS) 値 (0 ~ 7) に基づいて情報を表示します。 • label-number value : ダイナミック ラベル番号に基づいて情報を表示します。指定できる範囲は 158 ~ 255 です。 • policy-map <i>policy-map-name class-map class-map-name</i> : 指定されたポリシー マップとクラス マップの情報を表示します。 • asic number : (任意) ポートの ASIC 番号に基づいて情報を表示します。この番号は、常に 0 です。

policer { parameter-table qos-table selection-table } [asic number]	(任意) QoS 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。 <ul style="list-style-type: none"> • parameter-table : ポリサー パラメータ テーブルを表示します。 • qos-table : ポリサー QoS テーブルを表示します。 • selection-table : ポート割り当てテーブルを表示します。 • asic number : (任意) ポートの ASIC 番号に基づいて情報を表示します。この番号は、常に 0 です。
policy-map <i>policy-map-name</i> [asic number]	(任意) 指定されたポリシー マップの QoS 情報を表示します。 <ul style="list-style-type: none"> • asic number : (任意) ポートの ASIC 番号に基づいて情報を表示します。この番号は、常に 0 です。
port-class [asic number]	(任意) QoS ポートクラス テーブルを表示します。 <ul style="list-style-type: none"> • asic number : (任意) ポートの ASIC 番号に基づいて情報を表示します。この番号は、常に 0 です。
port-config <i>port-number</i> [asic number]	(任意) QoS ポート設定情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • <i>port-number</i> : 指定されたポート番号の QoS 設定を表示します。指定できる範囲は 0 ~ 25 です。 • asic number : (任意) ポートの ASIC 番号に基づいて情報を表示します。この番号は、常に 0 です。
port-info <i>port-number</i> [asic number]	(任意) QoS ポート情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • <i>port-number</i> : 指定されたポート番号の QoS 設定を表示します。指定できる範囲は 0 ~ 25 です。 • asic number : (任意) ポートの ASIC 番号に基づいて情報を表示します。この番号は、常に 0 です。
table-map <i>table-map-name</i> [asic number]	(任意) 指定されたテーブル マップの QoS 情報を表示します。 <ul style="list-style-type: none"> • asic number : (任意) ポートの ASIC 番号に基づいて情報を表示します。この番号は、常に 0 です。
vlan <i>vlan-id</i>	(任意) 指定された VLAN の QoS 情報を表示します。指定できる範囲は 1 ~ 4094 です。
statistics	QoS インターフェイス統計情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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

■ show platform qos

コマンド履歴

リリース	変更箇所
12.2(53)EX	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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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спан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。 <ul style="list-style-type: none"> 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 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。 <ul style="list-style-type: none"> hash-table : msm ハッシュ テーブルを表示します。 mac-address mac-address : 指定された MAC アドレスのテーブルを表示します。 vlan vlan-id : (任意) 指定された VLAN の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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の文字列です。

■ show platform resource-manager

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更箇所
	12.2(53)EX	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 sdflesh

Secure Digital (SD) フラッシュ メモリ カードの情報を表示するには **show platform sdflesh** 特権 EXEC コマンドを使用します。

```
show platform sdflesh [ | {begin | exclude | include} expression]
```

構文の説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 synchronization

プラットフォーム依存のスパニング ツリー ステート同期情報を表示するには **show platform spanning-tree synchronization** 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

detail	(任意) 詳細なスパニング ツリー同期情報を表示します。
vlan <i>vlan-id</i>	(任意) 指定された VLAN のスパニング ツリー同期情報を表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 status

プラットフォーム依存のステータス情報を表示するために **show platform status** 特権 EXEC コマンドを使用します。

```
show platform status [ | {begin | exclude | include} expression]
```

構文の説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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ンニング 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

<i>vlan-id</i>	指定された VLAN のスパンニング 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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 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 {handle number | log-results | table {acl | all | equal-cost-route | local
| mac-address | multicast-expansion | qos | secondary | 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 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]
```

```
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 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

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 qos secondary station vlan-list }	<p>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。</p> <ul style="list-style-type: none"> • 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。 • 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。 • 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] [invalid] [num number [detail [invalid]]] invalid]]	<p>情報を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • 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) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の文字列です。



(注) **ipv6**、**multicast-expansion**、および **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	変更箇所
	12.2(53)EX	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 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 {mapping | misc | mvid | refcount | rpc {receive | transmit}} [ |
  {begin | exclude | include} expression]
```

構文の説明

mapping	show platform vlan mapping コマンドを参照してください。
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。
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。 <ul style="list-style-type: none"> 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) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> 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)

prune キーワードは、コマンドラインのヘルプ スtring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	変更箇所
12.2(53)EX	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 vlan mapping

プラットフォームに依存する VLAN マッピング情報を表示するために **show platform vlan mapping** 特権 EXEC コマンドを使用します。

```
show platform vlan mapping [interface-id [vlan-id] | handle handle-id | usage] [ | {begin
| exclude | include} expression]
```

構文の説明

<i>interface-id</i>	(任意) 物理インターフェイス ID またはポート チャネル番号を入力します。ポート チャネル範囲は 1 ~ 48 です。
<i>vlan-id</i>	(任意) 回線上の元の VLAN の情報、カスタマー VLAN (C-VLAN) ID を表示します。VLAN ID の範囲は 1 ~ 4094 です。
handle <i>handle-id</i>	(任意) VLAN マッピング ハンドルの詳細を表示します。ハンドル ID の範囲は 0 ~ 65535 です。
usage	(任意) VLAN マッピング ハードウェア リソースの使用状況を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	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	変更箇所
12.2(53)EX	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

これらは show platform vlan mapping コマンドの出力例を示します。

```
Switch# show platform vlan mapping fastethernet 0/1
Platform Vlan Mapping Information
-----
Interface Fa0/1:
1-to-1
  option:      0
  cvlan:      10
  cvlanlist:  10
  cinnervlan:  0
  spvlan:    100 (0)
  spinnervlan: 0
  ingress block: 100
  egress block: 10
  hw state: on-hold
```

■ show platform vlan mapping

```

ingress handle: 0, egress handle: 1
ingress block handle: 2, egress block handle: 3

```

```

Switch# show platform vlan mapping handle 1
Platform Vlan Mapping Information
-----

```

```

Handle number: 1 Type: 1-to-1

```

```

Asic: 0 Region: Match 1 vlan

```

```

First entry: 977 Number of entries: 1

```

Index	TCAM ENTRY	TCAM MASK	DESCRIPTOR
977	7C006400 00000000	FE0FFF00 00004000	8010100A 00000000

```

Stat handle: 1 Packets: 0, Bytes: 0

```

```

Switch# show platform vlan mapping usage
Platform Vlan Mapping Information
-----

```

```

Port ASIC 0

```

Region Name	Min	Start	End	Used	Avail	Total	Percentage
Loopback	*	0	0	6	0	6	0%
Drop		0	6	492	0	486	0%
Match 2 vlans		0	492	976	0	484	0%
Match 1 vlan		0	976	1460	2	482	0%
Default operations		104	1460	1564	0	104	0%
Vlan blocking		0	1564	2048	2	482	0%

```

* = region needs compacting

```

```

Section Total

```

Start	End	Used	Avail	Total	Percentage
0	2048	4	2044	2048	0%



APPENDIX **C**

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](#)
aaa authorization network コマンド [2-28](#), [2-35](#), [2-37](#),
[2-39](#), [2-41](#), [2-43](#)
AAA 方式 [2-3](#)
ACE [2-126](#), [2-366](#)
ACL
 deny コマンド [2-124](#)
 IP [2-185](#)
 QoS クラスの一致基準として [2-326](#)
 許可 [2-364](#)
 非 IP プロトコル対応 [2-304](#)
 表示 [2-461](#)
 レイヤ 2 インターフェイス上 [2-185](#)
action コマンド [2-5](#)
alarm-contact コマンド [2-7](#)
alarm facility fcs-hysteresis コマンド [2-9](#)
alarm facility power-supply コマンド [2-10](#)
alarm facility temperature コマンド [2-11](#)
alarm profile
 作成 [2-13](#)
 表示 [2-465](#)
 ポートへの接続 [2-15](#)
alarm profile (インターフェイス コンフィギュレーション)
 コマンド [2-15](#)
alarm profile (グローバル コンフィギュレーション) コマ
 ンド [2-13](#)
alarm profile コンフィギュレーション モード [2-13](#)
alarm relay-mode コマンド [2-17](#)
alarm コマンド [2-13](#)
archive download-sw コマンド [2-18](#)
archive tar コマンド [2-21](#)

archive upload-sw コマンド [2-24](#)
arp access-list コマンド [2-26](#)
authentication control-direction コマンド [2-28](#)
authentication critical recovery delay コマンド [2-30](#)
authentication event コマンド [2-31](#)
authentication fallback コマンド [2-35](#)
authentication host-mode コマンド [2-37](#)
authentication mac-move permit コマンド [2-39](#)
authentication open コマンド [2-41](#)
authentication order コマンド [2-43](#)
authentication periodic コマンド [2-45](#)
authentication port-control コマンド [2-47](#)
authentication priority コマンド [2-49](#)
authentication timer コマンド [2-51](#)
authentication violation コマンド [2-53](#)
auth open コマンド [2-41](#)
auth order コマンド [2-43](#)
auth timer コマンド [2-51](#)

B

bandwidth コマンド [2-55](#)
boot config-file コマンド [2-58](#)
boot enable-break コマンド [2-59](#)
boot helper-config file コマンド [2-61](#)
boot helper コマンド [2-60](#)
boot manual コマンド [2-62](#)
boot private-config-file コマンド [2-63](#)
boot system コマンド [2-64](#)
boot (ブート ローダー) コマンド [A-3](#)
BPDU ガード、スパニング ツリー用 [2-707](#), [2-746](#)
BPDU フィルタリング、スパニング ツリー用 [2-705](#),
[2-746](#)

C

- cat (ブート ローダー) コマンド [A-5](#)
- CBWFQ、設定 [2-55](#)
- CDP、プロトコル トンネリングのイネーブル化 [2-282](#)
- CFM [2-352](#)
- channel-group コマンド [2-65](#)
- channel-protocol コマンド [2-69](#)
- CISP
 - 「Client Information Signalling Protocol」を参照
- class-map コマンド [2-73](#)
- class コマンド [2-71](#)
- clear ip arp inspection log コマンド [2-75](#)
- clear ip arp inspection statistics コマンド [2-76](#)
- clear ipc コマンド [2-79](#)
- clear ipv6 dhcp conflict コマンド [2-80](#)
- clear l2protocol-tunnel counters コマンド [2-81](#)
- clear lacp コマンド [2-82](#)
- clear logging onboard コマンド [2-83](#)
- clear mac address-table コマンド [2-84, 2-85](#)
- clear pagp コマンド [2-86, 2-90](#)
- clear policer cpu uni-eni counters コマンド [2-87](#)
- clear port-security コマンド [2-88](#)
- clear scada modbus tcp server statistics コマンド [2-91](#)
- clear spanning-tree counters コマンド [2-92](#)
- clear spanning-tree detected-protocols コマンド [2-93](#)
- clear vmps statistics コマンド [2-95](#)
- Client Information Signalling Protocol [2-133](#)
- conform-action コマンド [2-96](#)
- copy logging onboard module コマンド [2-98](#)
- copy (ブート ローダー) コマンド [A-6](#)
- CoS
 - QoS グループの一致基準として [2-327](#)
 - QoS 分類 [2-448](#)
 - ポリシー マップでの値の設定 [2-448](#)
- CoS 値、レイヤ 2 プロトコル パケットへの割り当て [2-286](#)
- CPU ASIC 統計、表示 [2-479](#)
- cpu traffic qos cos コマンド [2-100](#)

- cpu traffic qos dscp コマンド [2-104](#)
- cpu traffic qos precedence コマンド [2-109](#)
- cpu traffic qos qos-group コマンド [2-112](#)
- CPU 保護ポリサー、表示 [B-27](#)

D

- debug backup コマンド [3-2](#)
- debug dot1x コマンド [3-3](#)
- debug etherchannel コマンド [3-4](#)
- debug interface コマンド [3-7](#)
- debug ip dhcp snooping コマンド [3-8](#)
- debug ip igmp filter コマンド [3-9](#)
- debug ip igmp max-groups コマンド [3-10](#)
- debug ip igmp snooping コマンド [3-11](#)
- debug ip sla error twamp connection コマンド [3-12](#)
- debug ip sla error twamp control reflector コマンド [3-14](#)
- debug ip sla error twamp control server コマンド [3-16](#)
- debug ip sla trace twamp connection コマンド [3-20](#)
- debug ip verify source packet コマンド [3-28](#)
- debug lacp コマンド [3-29](#)
- debug mac-notification コマンド [3-30](#)
- debug matm move update コマンド [3-32](#)
- debug matm コマンド [3-31](#)
- debug monitor コマンド [3-33](#)
- debug mvrdbg コマンド [3-34](#)
- debug nvram コマンド [3-35](#)
- debug pagp コマンド [3-36](#)
- debug platform acl コマンド [3-37](#)
- debug platform backup interface コマンド [3-39](#)
- debug platform cfm コマンド [3-38](#)
- debug platform cpu-queues コマンド [3-40](#)
- debug platform dot1x コマンド [3-42](#)
- debug platform etherchannel コマンド [3-43](#)
- debug platform forw-tcam コマンド [3-44](#)
- debug platform ip arp inspection コマンド [3-45](#)
- debug platform ipc コマンド [3-54](#)
- debug platform ip dhcp コマンド [3-46](#)
- debug platform ip igmp snooping コマンド [3-47](#)

- debug platform ip multicast コマンド [3-49](#)
- debug platform ip source-guard コマンド [3-51](#)
- debug platform led コマンド [3-55](#)
- debug platform matm コマンド [3-56](#)
- debug platform messaging application コマンド [3-57](#)
- debug platform phy コマンド [3-58](#)
- debug platform pm コマンド [3-60](#)
- debug platform policer cpu uni-eni コマンド [3-62](#)
- debug platform port-asic コマンド [3-63](#)
- debug platform port-security コマンド [3-64](#)
- debug platform qos-acl-tcam コマンド [3-65](#)
- debug platform qos-manager コマンド [3-66](#)
- debug platform remote-commands コマンド [3-67](#)
- debug platform rep コマンド [3-68](#)
- debug platform resource-manager コマンド [3-69](#)
- debug platform snmp コマンド [3-70](#)
- debug platform span コマンド [3-71](#)
- debug platform supervisor-asic コマンド [3-72](#)
- debug platform sw-bridge コマンド [3-73](#)
- debug platform tcam コマンド [3-74](#)
- debug platform udld コマンド [3-76](#)
- debug platform vlan コマンド [3-77](#)
- debug pm コマンド [3-78](#)
- debug port-security コマンド [3-80](#)
- debug qos-manager コマンド [3-81](#)
- debug scada modbus tcp server コマンド [3-82](#)
- debug spanning-tree bpdu-opt コマンド [3-86](#)
- debug spanning-tree bpdu コマンド [3-85](#)
- debug spanning-tree mstp コマンド [3-87](#)
- debug spanning-tree switch コマンド [3-89](#)
- debug spanning-tree コマンド [3-83](#)
- debug sw-vlan ifs コマンド [3-93](#)
- debug sw-vlan notification コマンド [3-94](#)
- debug sw-vlan コマンド [3-91](#)
- debug udld コマンド [3-96](#)
- debug vqpc コマンド [3-98](#)
- defaultPort プロファイル [2-14, 2-15](#)
- define interface-range コマンド [2-114](#)
- delete コマンド [2-116](#)
- delete (ブート ロード) コマンド [A-7](#)
- deny (ARP アクセス リスト コンフィギュレーション) コマンド [2-117](#)
- deny (IPv6) コマンド [2-119](#)
- deny コマンド [2-124](#)
- DHCP スヌーピング
 - イネーブル化
 - VLAN 上 [2-216](#)
 - インターフェイス上で信頼 [2-214](#)
 - オプション 82 [2-208, 2-210](#)
 - 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 [2-210](#)
 - エラー回復タイマー [2-154](#)
 - レート制限 [2-213](#)
- 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 [2-77](#)
 - 更新 [2-415](#)
 - データベース エージェント、設定 [2-206](#)
 - バインディング
 - 削除 [2-204](#)
 - 追加 [2-204](#)
 - 表示 [2-553](#)
 - バインディング ファイル、設定 [2-206](#)
 - 表示
 - データベース エージェント ステータス [2-555, 2-557](#)
 - バインディング エントリ [2-553](#)
- diagnostic monitor コマンド [2-127](#)
- diagnostic schedule test コマンド [2-129](#)
- diagnostic start test コマンド [2-131](#)
- DiffServ コード ポイント
 - 「DSCP」を参照
- Digital Optical Monitoring
 - 「DoM」を参照
- dir (ブート ロード) コマンド [A-8](#)
- DoM
 - サポートされているトランシーバの表示 [2-544, 2-695, 2-696](#)
- dot1x credentials コマンド [2-133](#)

dot1x critical グローバル コンフィギュレーション コマンド [2-134](#)

dot1x default コマンド [2-135](#)

dot1x guest-vlan supplicant コマンド [2-136](#)

dot1x initialize コマンド [2-137](#)

dot1x max-reauth-req コマンド [2-138](#)

dot1x max-req コマンド [2-140](#)

dot1x pae コマンド [2-141](#)

dot1x supplicant force-multicast コマンド [2-143](#)

dot1x system-auth-control コマンド [2-144](#)

dot1x test eapol-capable コマンド [2-145](#)

dot1x test timeout コマンド [2-146](#)

dot1x timeout コマンド [2-147](#)

DSCP

QoS グループの一致基準として [2-328, 2-334](#)

QoS トラフィック マーキング用 [2-450](#)

ポリシー マップでの設定 [2-450](#)

duplex コマンド [2-150](#)

Dynamic Host Configuration Protocol (DHCP)

「DHCP スヌーピング」を参照

E

EAP-Request/Identity フレーム

再送信するまでの時間 [2-147](#)

送信する最高回数 [2-140](#)

E-LMI

イネーブル化 [2-158](#)

マッピング [2-160](#)

errdisable detect cause コマンド [2-152](#)

errdisable recovery コマンド [2-154](#)

errdisable インターフェイス、表示 [2-531](#)

errdisable 検出 [2-152](#)

EtherChannel

EtherChannel/PAgP のデバッグ、表示 [3-4](#)

LACP

channel-group 情報のクリア [2-82](#)

システム プライオリティ [2-289](#)

デバッグ メッセージ、表示 [3-29](#)

表示 [2-588](#)

プロトコルの制限 [2-69](#)

ホットスタンバイ ポートのポート プライオリティ [2-287](#)

モード [2-65](#)

PAgP

channel-group 情報のクリア [2-86](#)

エラー回復タイマー [2-154](#)

エラー検出 [2-152](#)

学習方式 [2-353](#)

集約ポート ラーナー [2-353](#)

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 [2-355](#)

デバッグ メッセージ、表示 [3-36](#)

表示 [2-634](#)

物理ポート ラーナー [2-353](#)

モード [2-65](#)

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 [2-65](#)

インターフェイス情報、表示 [2-531](#)

表示 [2-512](#)

負荷分散方式 [2-384](#)

プラットフォーム特定イベントのデバッグ、表示 [3-43](#)

ポート チャネル論理インターフェイスの作成 [2-179](#)

レイヤ 2 プロトコル トンネリングのイネーブル化

LACP [2-283](#)

PAgP [2-283](#)

UDLD [2-283](#)

ethernet evc コマンド [2-157](#)

ethernet lmi ce-vlan map コマンド [2-158, 2-160](#)

ethernet lmi global コマンド [2-158](#)

ethernet lmi コマンド [2-158](#)

ethernet loopback インターフェイス コンフィギュレーション コマンド [2-162](#)

ethernet loopback 特権 EXEC コマンド [2-165](#)

ethernet oam remote-failure コマンド [2-167](#)

ethernet uni id コマンド [2-171](#)

EVC [2-157](#)

UNI カウント [2-811](#)

VLAN [2-169](#)

サービス インスタンス [2-439](#)

EVC コンフィギュレーション モード [2-157](#)

EVC サービス

ポイントツーポイント [2-811](#)

ポイントツーマルチポイント [2-811](#)

exceed-action コマンド [2-172](#)

F

facility alarm relays、表示 [2-522](#)

facility alarm status、表示 [2-523](#)

fcs-threshold コマンド [2-174](#)

FCS ヒステリシスしきい値 [2-9](#)

FCS ビット エラー レート

設定 [2-174](#)

表示 [2-524](#)

変動しきい値 [2-9](#)

flash_init (ブート ロード) コマンド [A-10](#)

Flex Link

設定 [2-763](#)

表示 [2-531](#)

優先 VLAN の設定 [2-765](#)

flowcontrol コマンド [2-175](#)

format (ブート ロード) コマンド [A-11](#)

fsck (ブート ロード) コマンド [A-12](#)

H

help (ブート ロード) コマンド [A-13](#)

hw-module module logging onboard コマンド [2-177](#)

I

IEEE 802.1ag の接続障害管理

「CFM」を参照

IEEE 802.1Q トランク ポートおよびネイティブ VLAN [2-824](#)

IEEE 802.1Q トンネル ポート

制限 [2-771](#)

設定 [2-770](#)

表示 [2-500](#)

IEEE 802.1x

違反エラーの回復 [2-155](#)

スイッチポート モード [2-771](#)

「ポートベースの認証」も参照

IGMP グループ、最大値の設定 [2-221](#)

IGMP 最大グループ、デバッグ [3-10](#)

IGMP スヌーピング

querier [2-229](#)

イネーブル化 [2-225](#)

インターフェイスのトポロジ変更通知動作 [2-235](#)

クエリー要求 [2-233](#)

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 [2-239](#)

スイッチのトポロジ変更通知動作 [2-233](#)

設定可能脱退タイマーのイネーブル化 [2-227](#)

即時脱退機能のイネーブル化 [2-236](#)

表示 [2-561, 2-565, 2-567](#)

フラッディング クエリー カウント [2-233](#)

マルチキャスト テーブル [2-563](#)

レポート抑制 [2-231](#)

IGMP フィルタ

適用 [2-219](#)

デバッグ メッセージ、表示 [3-9](#)

IGMP プロファイル

作成 [2-223](#)

表示 [2-560](#)

interface port-channel コマンド [2-179](#)

interface range コマンド [2-181](#)

interface コマンド [2-183](#)

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 address コマンド [2-188](#)

- ip arp inspection filter vlan コマンド [2-190](#)
 - ip arp inspection limit コマンド [2-192](#)
 - ip arp inspection log-buffer コマンド [2-194](#)
 - ip arp inspection trust コマンド [2-196](#)
 - ip arp inspection validate コマンド [2-197](#)
 - ip arp inspection vlan logging コマンド [2-200](#)
 - ip arp inspection vlan コマンド [2-199](#)
 - ip dhcp snooping binding コマンド [2-204](#)
 - ip dhcp snooping database コマンド [2-206](#)
 - ip dhcp snooping information option allow-untrusted コマンド [2-210](#)
 - ip dhcp snooping information option format remote-id コマンド [2-212](#)
 - ip dhcp snooping information option コマンド [2-208](#)
 - ip dhcp snooping limit rate コマンド [2-213](#)
 - ip dhcp snooping trust コマンド [2-214](#)
 - ip dhcp snooping verify コマンド [2-215](#)
 - ip dhcp snooping vlan information option format-type circuit-id string コマンド [2-217](#)
 - ip dhcp snooping vlan コマンド [2-216](#)
 - ip dhcp snooping コマンド [2-203](#)
 - 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 [2-219](#)
 - ip igmp max-groups コマンド [2-221, 2-249, 2-251](#)
 - ip igmp profile コマンド [2-223](#)
 - ip igmp snooping last-member-query-interval コマンド [2-227](#)
 - ip igmp snooping querier コマンド [2-229](#)
 - ip igmp snooping report-suppression コマンド [2-231](#)
 - ip igmp snooping tcn flood コマンド [2-235](#)
 - ip igmp snooping tcn コマンド [2-233](#)
 - ip igmp snooping vlan immediate-leave コマンド [2-236](#)
 - ip igmp snooping vlan mrouter コマンド [2-237](#)
 - ip igmp snooping vlan static コマンド [2-239](#)
 - ip igmp snooping コマンド [2-225](#)
 - IP precedence、QoS グループの一致基準として [2-330](#)
 - ip source binding コマンド [2-245](#)
 - ip ssh コマンド [2-247](#)
 - ipv6 access-list コマンド [2-255](#)
 - ipv6 address dhcp コマンド [2-257](#)
 - ipv6 dhcp client request vendor コマンド [2-258](#)
 - ipv6 dhcp ping packets コマンド [2-259](#)
 - ipv6 dhcp pool コマンド [2-261](#)
 - ipv6 dhcp server コマンド [2-264](#)
 - ipv6 mld snooping last-listener-query count コマンド [2-268](#)
 - ipv6 mld snooping last-listener-query-interval コマンド [2-270](#)
 - ipv6 mld snooping listener-message-suppression コマンド [2-272](#)
 - ipv6 mld snooping robustness-variable コマンド [2-274](#)
 - ipv6 mld snooping tcn コマンド [2-276](#)
 - ipv6 mld snooping vlan コマンド [2-278](#)
 - ipv6 mld snooping コマンド [2-266](#)
 - IPv6 SDM テンプレート [2-436](#)
 - ipv6 traffic-filter コマンド [2-280](#)
 - IPv6 アクセス リスト、拒否条件 [2-119](#)
 - ip verify source コマンド [2-253](#)
 - IP アドレス、設定 [2-188](#)
 - IP アドレスの照合 [2-324](#)
 - IP 送信元ガード
 - イネーブル化 [2-253](#)
 - スタティック IP 送信元バインディング [2-245](#)
 - ディセーブル化 [2-253](#)
 - 表示
 - バインディング エントリ [2-574](#)
 - IP 送信元ガード、ダイナミック バインディング エントリの表示 [2-553](#)
 - IP ソース ガード
 - 表示する
 - 設定 [2-575](#)
 - IP マルチキャストアドレス [2-346](#)
-
- L**
 - l2protocol-tunnel cos コマンド [2-286](#)
 - l2protocol-tunnel コマンド [2-282](#)
 - LACP
 - 「EtherChannel」を参照

lacp port-priority コマンド [2-287](#)
 lacp system-priority コマンド [2-289](#)
 Layer 2 モード、イネーブル化 [2-759](#)
 Layer 3 モード、イネーブル化 [2-759](#)
 Link Aggregation Control Protocol
 「EtherChannel」を参照
 link state group コマンド [2-291](#)
 link state track コマンド [2-293](#)
 location (インターフェイス コンフィギュレーション) コマンド [2-296](#)
 location (グローバル コンフィギュレーション) コマンド [2-294](#)
 logging event power-inline-status コマンド [2-299](#)
 logging event コマンド [2-298](#)
 logging file コマンド [2-300](#)

M

mac access-group コマンド [2-302](#)
 mac access-list extended コマンド [2-304](#)
 mac address-table aging-time [2-302](#), [2-324](#)
 mac address-table aging-time コマンド [2-306](#)
 mac address-table learning コマンド [2-307](#)
 mac address-table move update コマンド [2-309](#)
 mac address-table notification コマンド [2-311](#)
 mac address-table static drop コマンド [2-314](#)
 mac address-table static コマンド [2-313](#)
 macro description コマンド [2-318](#)
 macro global description コマンド [2-321](#)
 macro global コマンド [2-319](#)
 macro name コマンド [2-322](#)
 MAC アクセス リスト [2-124](#)
 MAC アクセス リスト コンフィギュレーション モード [2-304](#)
 MAC アドレス
 MAC アドレス通知トラップのイネーブル化 [2-311](#)
 MAC アドレステーブル移行更新のイネーブル化 [2-309](#)
 VLAN ごとの MAC アドレス ラーニングのディセーブル化 [2-307](#)

照合 [2-324](#)
 スタティック
 インターフェイス上でドロップ [2-314](#)
 追加および削除 [2-313](#)
 表示 [2-621](#)
 テーブル [2-606](#)
 動的
 エージング タイム [2-306](#)
 削除 [2-84](#)
 表示 [2-612](#)
 表示
 MAC アドレス テーブル移行更新 [2-617](#)
 VLAN 単位 [2-623](#)
 VLAN のアドレス数 [2-610](#)
 インターフェイス単位 [2-614](#)
 エージング タイム [2-608](#)
 スタティック [2-621](#)
 スタティック エントリおよびダイナミック エントリ [2-604](#)
 すべて [2-606](#)
 通知設定 [2-616](#), [2-619](#)
 動的 [2-612](#)
 MAC アドレス グループ、表示 [2-602](#)
 MAC アドレス通知、デバッグ [3-30](#)
 match access-group コマンド [2-326](#)
 match cos コマンド [2-327](#)
 match ip dscp コマンド [2-328](#)
 match ip precedence コマンド [2-330](#)
 match qos-group コマンド [2-332](#)
 match vlan コマンド [2-334](#)
 Maximum Transmission Unit (最大伝送ユニット)
 「MTU」を参照
 mdix auto コマンド [2-337](#)
 media-type コマンド [2-339](#)
 memory (ブート ロード) コマンド [A-14](#)
 mkdir (ブート ロード) コマンド [A-15](#)
 MLD スヌーピング
 イネーブル化 [2-266](#)
 クエリーの設定 [2-268](#), [2-270](#)

- 設定 [2-272, 2-274](#)
- トポロジ変更通知の設定 [2-276](#)
- MODBUS
 - 「scada modbus tcp server」を参照
- monitor session コマンド [2-341](#)
- more (ブート ロoader) 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 [2-724](#)
 - VLAN とインスタンス間のマッピング [2-724](#)
 - 現在または保留中の構成の表示 [2-725](#)
 - コンフィギュレーション リビジョン番号 [2-725](#)
 - 設定名 [2-724](#)
 - 表示 [2-664](#)
 - 変更の中止 [2-724](#)
 - 変更の適用 [2-724](#)
 - ステート情報の表示 [2-663](#)
 - ステート変更
 - BPDU ガードのイネーブル化 [2-707, 2-746](#)
 - BPDU フィルタリングのイネーブル化 [2-705, 2-746](#)
 - PortFast 対応ポートのシャットダウン [2-746](#)
 - Port Fast のイネーブル化 [2-746, 2-749](#)
 - 転送遅延時間 [2-729](#)
 - フォワーディング ステートへの高速移行 [2-718](#)
 - 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 [2-749](#)
 - リスニングおよびラーニング ステートの期間 [2-729](#)
 - 相互運用 [2-93](#)
 - パス コスト [2-727](#)
 - 表示 [2-664](#)
 - プロトコル移行プロセスの再開 [2-93](#)
 - プロトコル モード [2-722](#)
 - リンク タイプ [2-718](#)
 - ルート スイッチ
 - BPDU ドロップまでの最大ホップ数 [2-735](#)
 - BPDU メッセージの間隔 [2-733](#)
 - hello BPDU メッセージの間隔 [2-731, 2-742](#)
 - hello タイム [2-731, 2-742](#)
 - 拡張システム ID の影響 [2-713](#)
 - スイッチのプライオリティ [2-740](#)
 - 選択に関するポート プライオリティ [2-737](#)
 - プライマリまたはセカンダリ [2-742](#)
 - 有効期限 [2-733](#)
 - ルート ポート
 - 指定ポートの制限 [2-715](#)
 - ルート ガード [2-715](#)
 - ルートとなるポートの制限 [2-715](#)
 - ループ ガード [2-715](#)
- MTU
 - グローバル設定の表示 [2-671](#)
 - サイズの設定 [2-793](#)
- Multicast Listener Discovery
 - 「MLD」を参照
- Multicast VLAN、MVR [2-347](#)
- 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 [2-347](#)
 - インターフェイス情報の表示 [2-630](#)
 - インターフェイスの設定 [2-349](#)
 - 設定 [2-346](#)
 - デバッグ メッセージ、表示 [3-34](#)
 - 表示 [2-628](#)
 - メンバー、表示 [2-632](#)
- mvr vlan group コマンド [2-350](#)
- mvr (インターフェイス コンフィギュレーション) コマンド [2-349](#)
- mvr (グローバル コンフィギュレーション) コマンド [2-346](#)

N

nonegotiate、速度 [2-754, 2-755](#)

notifies コマンド [2-13](#)
no vlan コマンド [2-818](#)

O

OAM PDU [2-167](#)
oam protocol cfm svlan コマンド [2-352](#)
OAM プロトコル [2-352](#)
OAM プロトコルとしての CFM [2-352](#)

P

PAgP
「EtherChannel」を参照
pagp learn-method コマンド [2-353](#)
pagp port-priority コマンド [2-355](#)
permit (ARP アクセス リスト コンフィギュレーション) コマンド [2-357](#)
permit (IPv6) コマンド [2-359](#)
permit コマンド [2-364](#)
Per-VLAN Spanning-Tree Plus
「STP」を参照
PID の表示 [2-547](#)
PIM-DVMRP、マルチキャスト ルータ学習方式 [2-237](#)
PoE
エラー回復タイマー [2-154](#)
エラー検出 [2-152](#)
コントローラ レジスタ値の表示 [2-488](#)
状態のロギング [2-299](#)
電力管理情報の表示 [2-652](#)
電力管理モードの設定 [2-388](#)
電力消費のポリシング [2-393](#)
電力設定 [2-391](#)
電力のモニタリング [2-393](#)
police aggregate コマンド [2-377](#)
policer aggregate コマンド [2-372](#)
policer cpu uni コマンド [2-379](#)
police コマンド [2-367](#)
policy-map コマンド [2-381](#)

Port Aggregation Protocol
「EtherChannel」を参照
port-channel load-balance コマンド [2-384](#)
PortFast、スパニング ツリー用 [2-749](#)
port-type コマンド [2-386](#)
power inline consumption コマンド [2-391](#)
power inline police コマンド [2-393](#)
power inline コマンド [2-388](#)
Power over Ethernet
「PoE」を参照
priority コマンド [2-396](#)
private-vlan mapping コマンド [2-402](#)
private-vlan コマンド [2-399](#)
PVST+
「STP」を参照

Q

QoS
違反アクション、設定 [2-816](#)
クラス マップ
一致基準の定義 [2-327](#)
作成 [2-73](#)
表示 [2-478](#)
集約ポリサー
作成 [2-372](#)
適用 [2-377](#)
表示 [2-638](#)
超過アクション、設定 [2-173](#)
テーブル マップ
設定 [2-795](#)
表示 [2-672](#)
適合アクション、設定 [2-97](#)
統計情報の表示 [2-642, B-36](#)
ポリシー マップ
CoS 値の設定 [2-448](#)
DSCP 値の設定 [2-450](#)
IP precedence 値の設定 [2-452](#)
QoS グループ ID の設定 [2-454](#)

インターフェイスへの適用 [2-443](#), [2-456](#)

作成 [2-381](#)

集約ポリサーの適用 [2-372](#), [2-377](#), [2-379](#), [2-445](#)

トラフィックの分類 [2-71](#)

ポリサーの定義 [2-367](#)

ポリシー マップの表示 [2-642](#)

QoS 一致基準

ACL [2-326](#)

CoS 値 [2-327](#)

DSCP 値 [2-328](#), [2-334](#)

precedence 値 [2-330](#)

QoS グループ番号 [2-332](#)

QoS グループ

QoS トラフィック分類用 [2-454](#)

一致基準として [2-332](#)

ポリシー マップでの設定 [2-454](#)

QoS ポリサーの認定情報レート [2-368](#), [2-372](#)

Quality Of Service

「QoS」を参照

queue-limit コマンド [2-404](#)

R

radius-server dead-criteria コマンド [2-407](#)

radius-server host コマンド [2-409](#)

Rapid Per-VLAN Spanning-Tree Plus

「STP」を参照

Rapid PVST+

「STP」を参照

relay-major コマンド [2-13](#)

relay-minor コマンド [2-13](#)

reload コマンド [2-411](#)

remote-span コマンド [2-413](#)

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

rename (ブートローダー) コマンド [A-17](#)

renew ip dhcp snooping database コマンド [2-415](#)

rep admin vlan コマンド [2-417](#)

rep block port コマンド [2-418](#)

rep lsl-age-timer コマンド [2-421](#)

rep preempt delay コマンド [2-423](#)

rep preempt segment コマンド [2-425](#)

rep segment コマンド [2-426](#)

rep stcn コマンド [2-429](#)

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 [2-433](#)

RSPAN

remote-span コマンド [2-413](#)

RSPAN トラフィックのフィルタリング [2-341](#)

セッション

新しく開始 [2-341](#)

インターフェイスの追加 [2-341](#)

表示 [2-625](#)

設定 [2-341](#)

表示 [2-625](#)

S

scada modbus tcp server [2-434](#)

sd_init (ブートローダー) コマンド [A-20](#)

sdm prefer コマンド [2-436](#)

SDM テンプレート

許容されるリソース [2-437](#)

デュアル IPv4 および IPv6 [2-436](#)

表示 [2-661](#)

service password-recovery コマンド [2-441](#)

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 [2-443](#)

service policy (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 [2-445](#)

service-policy 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 [2-445](#)

set cos コマンド [2-448](#)

set dscp コマンド [2-450](#)

set precedence コマンド [2-452](#)

set qos-group コマンド [2-454](#)

- setup コマンド [2-456](#)
- set (ブート ローダー) コマンド [A-21](#)
- SFP、情報の表示 [2-547](#)
- shape average コマンド [2-459](#)
- show access-lists コマンド [2-461](#)
- show aggregate-policer コマンド [2-672](#)
- show alarm description port コマンド [2-464](#)
- show alarm profile コマンド [2-465](#)
- show alarm settings コマンド [2-467](#)
- show archive status コマンド [2-468](#)
- show arp access-list コマンド [2-469](#)
- show authentication コマンド [2-470](#)
- show boot コマンド [2-474](#)
- show class-map コマンド [2-478](#)
- show controllers cpu-interface コマンド [2-479](#)
- show controllers ethernet-controller コマンド [2-481](#)
- show controllers power inline コマンド [2-488](#)
- show controllers team コマンド [2-490](#)
- show controllers utilization コマンド [2-492](#)
- show cpu traffic qos コマンド [2-494](#)
- show diagnostic コマンド [2-496](#)
- show dot1q-tunnel コマンド [2-500](#)
- show dot1x コマンド [2-501](#)
- show env コマンド [2-504](#)
- show errdisable detect コマンド [2-506](#)
- show errdisable flap-values コマンド [2-508](#)
- show errdisable recovery コマンド [2-510](#)
- show etherchannel コマンド [2-512](#)
- show ethernet loopback コマンド [2-515](#)
- show ethernet service evc コマンド [2-517](#)
- show ethernet service instance コマンド [2-518](#)
- show ethernet service interface コマンド [2-520](#)
- show facility-alarm relay コマンド [2-522](#)
- show facility-alarm status コマンド [2-523](#)
- show fcs threshold コマンド [2-524](#)
- show flowcontrol コマンド [2-526](#)
- show idprom コマンド [2-528](#)
- show interface rep コマンド [2-542](#)
- show interfaces counters コマンド [2-540](#)
- show interfaces rep コマンド [2-542](#)
- show interfaces コマンド [2-531](#)
- show interface transceivers コマンド [2-544](#)
- show inventory コマンド [2-547](#)
- show ip arp inspection コマンド [2-548](#)
- show ipc コマンド [2-577](#)
- show ip dhcp snooping binding コマンド [2-553](#)
- show ip dhcp snooping database コマンド [2-555, 2-557](#)
- show ip dhcp snooping コマンド [2-552](#)
- show ip igmp profile コマンド [2-560](#)
- show ip igmp snooping groups コマンド [2-563](#)
- show ip igmp snooping mrouter コマンド [2-565](#)
- show ip igmp snooping querier detail コマンド [2-567](#)
- show ip igmp snooping querier コマンド [2-567](#)
- show ip igmp snooping コマンド [2-561](#)
- show ip igmp snooping コマンド クエリアの詳細 [2-567](#)
- show ip sla standards コマンド [2-569](#)
- show ip sla twamp connection コマンド [2-494](#)
- show ip source binding コマンド [2-574](#)
- show ipv6 access-list コマンド [2-581](#)
- show ipv6 dhcp conflict コマンド [2-583](#)
- show ipv6 route updated コマンド [2-584](#)
- show ip verify source コマンド [2-575](#)
- show l2protocol-tunnel コマンド [2-586](#)
- show lacp コマンド [2-588](#)
- show link state group コマンド [2-592](#)
- show lldp コマンド [2-594](#)
- show location コマンド [2-595](#)
- show logging onboard コマンド [2-598](#)
- show mac access-group コマンド [2-602](#)
- show mac address-table address コマンド [2-606](#)
- show mac address-table aging time コマンド [2-608](#)
- show mac address-table count コマンド [2-610](#)
- show mac address-table dynamic コマンド [2-612](#)
- show mac address-table interface コマンド [2-614](#)
- show mac address-table learning コマンド [2-616](#)
- show mac address-table move update コマンド [2-617](#)
- show mac address-table notification コマンド [2-85, 2-619, 3-32](#)

- show mac address-table static コマンド [2-621](#)
- show mac address-table vlan コマンド [2-623](#)
- show mac address-table コマンド [2-604](#)
- show monitor コマンド [2-625](#)
- show mvr interface コマンド [2-630](#)
- show mvr members コマンド [2-632](#)
- show mvr コマンド [2-628](#)
- show pagp コマンド [2-634](#)
- show parser macro コマンド [2-636](#)
- show platform acl コマンド [B-2](#)
- show platform backup interface コマンド [B-3](#)
- show platform cfm コマンド [B-4](#)
- show platform configuration コマンド [B-5](#)
- show platform dl コマンド [B-6](#)
- show platform etherchannel コマンド [B-7](#)
- show platform forward コマンド [B-8](#)
- show platform frontend-controller コマンド [B-10](#)
- show platform igmp snooping コマンド [B-11](#)
- show platform ipc trace コマンド [B-16](#)
- show platform ip multicast コマンド [B-13](#)
- show platform ip unicast コマンド [B-14](#)
- show platform ipv6 unicast コマンド [B-17](#)
- show platform l2pt dm コマンド [B-19](#)
- show platform layer4op コマンド [B-20, B-44](#)
- show platform mac-address-table コマンド [B-21](#)
- show platform messaging コマンド [B-22](#)
- show platform monitor コマンド [B-23](#)
- show platform mvr table コマンド [B-24](#)
- show platform pm コマンド [B-25](#)
- show platform policer cpu コマンド [B-27](#)
- show platform port-asic コマンド [B-31](#)
- show platform port-security コマンド [B-35](#)
- show platform qos コマンド [B-36](#)
- show platform resource-manager コマンド [B-39](#)
- show platform sdfsflash [B-41](#)
- show platform snmp counters コマンド [B-42](#)
- show platform spanning-tree synchronization コマンド [B-43](#)
- show platform stp-instance コマンド [B-45](#)
- show platform tcam コマンド [B-46](#)
- show platform vlan mapping コマンド [B-49](#)
- show platform vlan コマンド [B-48](#)
- show policer aggregate コマンド [2-638](#)
- show policer cpu uni-eni コマンド [2-639](#)
- show policy-map interface の出力フィールド [2-645](#)
- show policy-map コマンド [2-642](#)
- show port security コマンド [2-647](#)
- show port-type コマンド [2-650](#)
- show power inline コマンド [2-652](#)
- show rep topology コマンド [2-657](#)
- show scada modbus tcp server コマンド [2-660](#)
- show sdm prefer コマンド [2-661](#)
- show spanning-tree コマンド [2-663](#)
- show storm-control コマンド [2-669](#)
- show system mtu コマンド [2-671](#)
- show uddl コマンド [2-674](#)
- show version コマンド [2-676](#)
- show vlan access-map コマンド [2-683](#)
- show vlan filter コマンド [2-684](#)
- show vlan mapping コマンド [2-685](#)
- show vlan コマンド [2-678](#)
- show vlan コマンド、フィールド [2-680](#)
- show vmps コマンド [2-687](#)
- shutdown vlan コマンド [2-690](#)
- shutdown コマンド [2-689](#)
- snmp mib rep trap-rate コマンド [2-691](#)
- snmp-server enable traps コマンド [2-692](#)
- snmp-server host コマンド [2-697](#)
- snmp trap mac-notification change コマンド [2-701](#)
- SNMP 通知、送信のイネーブル [2-692](#)
- SNMP トラップ
 - MAC アドレス通知機能のイネーブル化 [2-311](#)
 - MAC アドレス通知トラップのイネーブル化 [2-701](#)
 - 送信のイネーブル化 [2-692](#)
- SNMP ホスト、指定 [2-697](#)
- SPAN
 - SPAN トラフィックのフィルタリング [2-341](#)

- セッション
 - インターフェイスへの追加 [2-341](#)
 - 新規に開始 [2-341](#)
 - 表示 [2-625](#)
- 設定 [2-341](#)
- デバッグ メッセージ、表示 [3-33](#)
- 表示 [2-625](#)
- spanning-tree bpdudfilter コマンド [2-703, 2-705](#)
- spanning-tree bpduguard コマンド [2-707](#)
- spanning-tree cost コマンド [2-709](#)
- spanning-tree etherchannel コマンド [2-711](#)
- spanning-tree extend system-id コマンド [2-713](#)
- spanning-tree guard コマンド [2-715](#)
- spanning-tree link-type コマンド [2-718](#)
- spanning-tree loopguard default コマンド [2-720](#)
- spanning-tree mode コマンド [2-722](#)
- spanning-tree mst configuration コマンド [2-724](#)
- spanning-tree mst cost コマンド [2-727](#)
- spanning-tree mst forward-time コマンド [2-729](#)
- spanning-tree mst hello-time コマンド [2-731](#)
- spanning-tree mst max-age コマンド [2-733](#)
- spanning-tree mst max-hops コマンド [2-735](#)
- spanning-tree mst port-priority コマンド [2-737](#)
- spanning-tree mst pre-standard コマンド [2-739](#)
- spanning-tree mst priority コマンド [2-740](#)
- spanning-tree mst root コマンド [2-742](#)
- 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 [2-749](#)
- spanning-tree portfast (グローバル コンフィギュレーション) コマンド [2-746](#)
- spanning-tree port-priority コマンド [2-744](#)
- Spanning Tree Protocol (スパニング ツリー プロトコル)
 - 「STP」を参照
- spanning-tree vlan コマンド [2-751](#)
- speed コマンド [2-754](#)
- SSH、バージョンの設定 [2-247](#)
- storm-control コマンド [2-756](#)
- STP
 - ENI でのイネーブル化 [2-703](#)
 - EtherChannel の設定矛盾 [2-711](#)
 - VLAN オプション [2-740, 2-751](#)
 - カウンタ、クリア [2-92](#)
 - 拡張システム ID [2-713](#)
 - ステート情報の表示 [2-663](#)
 - ステート変更
 - BPDU ガードのイネーブル化 [2-707, 2-746](#)
 - BPDU フィルタリングのイネーブル化 [2-705, 2-746](#)
 - PortFast 対応ポートのシャットダウン [2-746](#)
 - Port Fast のイネーブル化 [2-746, 2-749](#)
 - エラー ステートから回復するタイマーのイネーブル化 [2-154](#)
 - 転送遅延時間 [2-751](#)
 - 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 [2-749](#)
 - リスニングおよびラーニング ステートの期間 [2-751](#)
 - デバッグ メッセージ、表示
 - MSTP [3-87](#)
 - 最適化された BPDU 処理 [3-86](#)
 - スイッチ シム [3-89](#)
 - スパニングツリーのアクティビティ [3-83](#)
 - 送受信された BPDU [3-85](#)
 - パス コスト [2-709](#)
 - プロトコル トンネリングのイネーブル化 [2-282](#)
 - プロトコル モード [2-722](#)
 - ルート スイッチ
 - BPDU メッセージの間隔 [2-751](#)
 - hello BPDU メッセージの間隔 [2-751](#)
 - hello タイム [2-751](#)
 - 拡張システム ID の影響 [2-713, 2-752](#)
 - スイッチのプライオリティ [2-751](#)
 - 選択に関するポート プライオリティ [2-744](#)
 - プライマリまたはセカンダリ [2-751](#)
 - 有効期限 [2-751](#)
 - ルート ポート
 - 指定ポートの制限 [2-715](#)
 - ルート ガード [2-715](#)
 - ルートとなるポートの制限 [2-715](#)

ループガード 2-715

STP の拡張システム ID 2-713

SVI、作成 2-183

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 2-761

switchport backup interface コマンド 2-763

switchport block コマンド 2-767

switchport host コマンド 2-769

switchport mode private-vlan コマンド 2-773

switchport mode コマンド 2-770

switchport port-security aging コマンド 2-780

switchport port-security コマンド 2-776

switchport private-vlan コマンド 2-782

switchport protected コマンド 2-785

switchport trunk コマンド 2-787

switchport vlan mapping コマンド 2-789

switchport コマンド 2-759

syslog コマンド 2-13

system env temperature threshold yellow コマンド 2-792

system mtu コマンド 2-793

T

table-map コマンド 2-795

tar ファイル、作成、一覧表示、および抽出 2-21

TDR、実行 2-797

test cable-diagnostics tdr コマンド 2-797

traceroute mac ip コマンド 2-802

traceroute mac コマンド 2-799

type (ブート ローダー) コマンド A-24

U

UDLD

アグレッシブ モード 2-804, 2-806

インターフェイスごとのイネーブル化 2-806

エラー回復タイマー 2-155

グローバルにイネーブル化 2-804

シャットダウン インターフェイスのリセット 2-809

ステータス 2-674

デバッグ メッセージ、表示 3-96

ノーマル モード 2-804, 2-806

メッセージ タイマー 2-804

udld port コマンド 2-806

udld reset コマンド 2-809

udld コマンド 2-804

UNI

イーサネット 2-169

バンドルおよび多重化 2-169

uni count コマンド 2-811

UniDirectional Link Detection (単方向リンク検出)

「UDLD」を参照

UNI ID、イーサネット 2-171

uni-vlan コマンド 2-813

unset (ブート ローダー) コマンド A-25

V

version (ブート ローダー) コマンド A-27

violate-action コマンド 2-815

VLAN

MAC アドレス

数 2-610

表示 2-623

拡張範囲 2-818

再起動 2-690

シャットダウン 2-690

設定 2-818

設定の表示 2-678

設定の保存 2-818

中断 2-690

追加 2-818

デバッグ メッセージ、表示

VLAN IOS File System エラー テスト 3-93

VLAN マネージャのアクティビティ 3-91

- アクティベーション **3-94**
 - 標準範囲 **2-818**
 - プライベート **2-773**
 - 設定 **2-399**
 - 表示 **2-678**
 - 「プライベート VLAN」も参照
 - vlan access-map コマンド **2-822**
 - vlan dot1q tag native コマンド **2-824**
 - vlan filter コマンド **2-826**
 - VLAN ID 範囲 **2-818**
 - VLAN ID 変換
 - 「VLAN マッピング」を参照
 - VLAN Query Protocol
 - 「VQP」を参照
 - VLAN アクセス マップ
 - アクション **2-5**
 - 表示 **2-683**
 - VLAN アクセス マップ コンフィギュレーション モード **2-822**
 - vlan コマンド **2-818**
 - VLAN コンフィギュレーション モード
 - 開始 **2-818**
 - 概要 **1-2**
 - コマンド **2-818**
 - 説明 **1-4**
 - VLAN での MLD スヌーピング、イネーブル化 **2-278**
 - VLAN フィルタ、表示 **2-684**
 - VLAN マッピング
 - 設定 **2-789**
 - 説明 **2-790**
 - 表示 **2-685**
 - VLAN マップ
 - 作成 **2-822**
 - 定義 **2-324**
 - 適用 **2-826**
 - 表示 **2-683**
 - VMPS
 - エラー回復タイマー **2-155**
 - サーバの設定 **2-831**
 - ダイナミック VLAN 割り当ての再確認 **2-828**
 - 表示 **2-687**
 - vmmps reconfirm (グローバル コンフィギュレーション) コマンド **2-829**
 - vmmps reconfirm (特権 EXEC) コマンド **2-828**
 - vmmps retry コマンド **2-830**
 - vmmps server コマンド **2-831**
 - VQP
 - クライアント統計情報のクリア **2-95**
 - サーバごとの再試行回数 **2-830**
 - 再確認間隔 **2-829**
 - 情報の表示 **2-687**
 - ダイナミック VLAN 割り当ての再確認 **2-828**
 - ダイナミック アクセス ポート **2-762**
 - VTP、トンネリングのイネーブル化 **2-282**
-
- ## W
- Weighted Tail Drop
 - 「WTD」を参照
 - WTD、queue-limit コマンド **2-404**
-
- ## あ
- アクセス グループ
 - IP **2-185**
 - MAC、表示 **2-602**
 - QoS 分類のマッチング **2-326**
 - 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 ポート **2-770**
 - アクセス モード **2-770**
 - アクセス リスト、IPv6 **2-255**
 - アップグレード
 - ソフトウェア イメージ **2-18**
 - ステータスのモニタリング **2-468**

アドレスのエイリアス [2-347](#)

アラーム ID [2-14](#), [2-464](#)

アラーム接点ステータス、表示 [2-504](#)

い

イーサネット UNI コンフィギュレーション [2-169](#)

イーサネット仮想接続

「EVC」を参照

イーサネット コントローラ、内部レジスタの表示 [2-481](#)

イーサネット サービス

デバッグ [3-5](#)

表示 [2-517](#)

イーサネット サービス インスタンス [2-439](#)

イーサネット サービス インターフェイス [2-520](#)

イーサネット統計情報、収集 [2-433](#)

イーサネット ローカル管理インターフェイス

「E-LMI」を参照

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 [2-614](#)

イーサネット インターフェイスのチャンネル グループへの割り当て [2-65](#)

再起動 [2-689](#)

設定 [2-150](#)

ディセーブル化 [2-689](#)

デバッグ メッセージ、表示 [3-7](#)

複数の設定 [2-181](#)

ポート チャネル論理の作成 [2-179](#)

インターフェイス コンフィギュレーション モード [1-2](#), [1-4](#)

インターフェイスの速度、設定 [2-754](#)

インターフェイス範囲マクロ [2-114](#)

インターフェイスへのポリシー マップの付加 [2-443](#)

う

運用管理および保守プロトコル

「OAM」を参照

え

エラー条件、表示 [2-508](#)

お

オペレーティング システム、リロード [2-411](#)

親ポリシー マップ [2-446](#)

温度アラーム、設定 [2-11](#)

温度情報、表示 [2-504](#)

温度ステータス、表示 [2-504](#)

オンボード障害ロギング、イネーブル化 [2-177](#)

オンボード障害ロギング、表示 [2-598](#)

オンライン診断

イネーブル化

スケジューリング [2-129](#)

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 [2-129](#)

テストベースのテストの設定 [2-129](#)

スケジューリングの削除 [2-129](#)

スケジュールされたスイッチオーバー

イネーブル化 [2-129](#)

ディセーブル化 [2-129](#)

テストの開始 [2-131](#)

テストの間隔の設定 [2-129](#)

オンライン診断テスト、開始 [2-131](#)

オンライン診断テスト、結果の表示 [2-496](#)

か

外部アラーム、設定 [2-7](#)

回復メカニズム

原因 [2-154](#)

タイマーの間隔 [2-155](#)
 表示 [2-476, 2-506, 2-510](#)
 拡張範囲 VLAN
 許可 VLAN リスト [2-787](#)
 設定 [2-818](#)
 環境アラーム、表示 [2-467](#)
 環境変数、表示 [2-474](#)

き

起動
 Cisco IOS イメージ [2-64](#)
 環境変数の表示 [2-474](#)
 手動 [2-62](#)
 中断 [2-59](#)
 許可 VLAN [2-787](#)

く

クエリー時間、MVR [2-346](#)
 クラスベース均等化キューイング
 「CBWFQ」を参照
 クラスベース トラフィック シェーピング [2-459](#)
 クラス マップ
 一致基準の定義 [2-327](#)
 作成 [2-73](#)
 表示 [2-478](#)
 クラスマップ
 一致 [2-73](#)
 クラスマップ コンフィギュレーション モード [2-73](#)
 クリティカル VLAN [2-31](#)
 グローバル コンフィギュレーション モード [1-2, 1-3](#)

こ

子ポリシー マップ [2-445](#)
 混合ポート、プライベート VLAN [2-773](#)
 コントロールプレーンセキュリティ [2-379](#)

コントロールプレーン統計情報、クリア [2-87](#)
 コントロールプレーンのポリサー情報、表示 [2-639](#)
 コントロールプレーン ポリサー [2-87](#)
 コンフィギュレーション ファイル
 名前の指定 [2-58, 2-63](#)
 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 インスタンス コマンド [2-439](#)
 サービス インスタンス、表示 [2-518](#)
 サービス クラス
 「CoS」を参照
 再認証
 試行間隔 [2-147](#)

し

システム メッセージのログ [2-299](#)
 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 [2-300](#)
 システム リソース テンプレート [2-436](#)
 自動ネゴシエーション、デプレックス モードの [2-151](#)
 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 [2-282](#)
 ジャンボ フレーム
 「MTU」を参照
 集約ポート ラーナー [2-353](#)
 集約ポリサー
 QoS [2-374](#)
 作成 [2-372](#)
 適用 [2-377](#)
 表示 [2-638](#)
 受信、フロー制御パケットの [2-175](#)
 出力ポリシー マップ
 および QoS グループ分類 [2-332](#)
 キュー制限 [2-404](#)
 サポートされていないコマンド [2-382](#)
 設定時の注意事項 [2-382](#)

トラフィック シェーピング [2-459](#)

プライオリティ [2-397](#)

障害ロギング データ

クリア [2-83](#)

コピー [2-98](#)

診断テストのスケジューリング [2-129](#)

す

スイッチポート、表示 [2-531](#)

スイッチング、特徴

インターフェイスに戻る [2-759](#)

変更 [2-759](#)

スケジュールされたスイッチオーバー

イネーブル化 [2-129](#)

ディセーブル化 [2-129](#)

スタティック アクセス ポート、設定 [2-761](#)

スティッキ ラーニング、イネーブル化 [2-776](#)

せ

製品識別情報の表示 [2-547](#)

セカンダリ温度アラーム [2-11](#)

セキュア ポート、制限 [2-778](#)

設定、複数のインターフェイスの [2-181](#)

そ

送信、フロー制御パケットの [2-175](#)

送信元ポート、MVR [2-349](#)

即時脱退機能、MVR [2-349](#)

即時脱退処理 [2-236](#)

即時脱退処理、IPv6 [2-278](#)

ソフトウェア イメージ

アップグレード [2-18](#)

アップロード [2-24](#)

削除 [2-116](#)

ダウンロード [2-18](#)

ソフトウェア バージョン、表示 [2-676](#)

た

帯域幅、QoS の設定 [2-55](#)

ダイナミック ARP 検査

ARP ACL

VLAN に適用 [2-190](#)

定義 [2-26](#)

パケットの許可 [2-357](#)

パケットの拒否 [2-117](#)

表示 [2-469](#)

clear

統計情報 [2-76](#)

VLAN 単位でイネーブル化 [2-199](#)

インターフェイスの信頼状態 [2-196](#)

エラー回復タイマー [2-154](#)

エラー検出 [2-152](#)

記録するパケットのタイプ [2-200](#)

クリア

ログ バッファ [2-75](#)

検証チェック [2-197](#)

着信 ARP パケットのレート制限 [2-192](#)

統計情報

クリア [2-76](#)

表示 [2-548](#)

表示

ARP ACL [2-469](#)

信頼状態およびレート制限 [2-548](#)

設定および動作ステート [2-548](#)

統計情報 [2-548](#)

ログ バッファ [2-548](#)

ログ バッファ

クリア [2-75](#)

設定 [2-194](#)

表示 [2-548](#)

ダイナミック アクセス ポート

制限 [2-762](#)

設定 [2-761](#)

多重化、UNI [2-169](#)
 弾力的、認証、順序付け [2-43](#)

て

定義済みのコマンド モード [1-1](#)
 ディレクトリ、削除 [2-116](#)
 テーブル マップ
 QoS [2-795](#)
 設定 [2-795](#)
 表示 [2-672](#)
 テーブルマップ コンフィギュレーション モード [2-795](#)
 デュアル IPv4/IPv6 テンプレート [2-359](#)
 デュアルパーパス アップリンク ポート、タイプの選
 択 [2-339](#)
 電源アラーム、設定 [2-10](#)
 電源情報、表示 [2-504](#)
 電源ステータス、表示 [2-504](#)
 転送結果の表示 [B-8](#)
 テンプレート、システム リソース [2-436](#)

と

統計情報、イーサネット グループ [2-433](#)
 特権 EXEC モード [1-2, 1-3](#)
 ドメイン、CFM [2-352](#)
 トラフィック シェーピング、QoS [2-459](#)
 トランキング、VLAN モード [2-770](#)
 トランク ポート [2-770](#)
 トランク モード [2-770](#)
 ドロップしきい値、レイヤ 2 プロトコル トンネリ
 ング [2-282](#)
 トンネル ポート、レイヤ 2 プロトコル、表示 [2-586](#)

な

内部レジスタ、表示 [2-481, 2-490](#)

に

入力ポリシー マップ
 および ACL 分類 [2-326](#)
 および集約ポリサー [2-374](#)
 サポートされていないコマンド [2-382](#)
 設定時の注意事項 [2-382](#)

ね

ネイティブ VLAN [2-787](#)
 ネイティブ VLAN タギング [2-824](#)
 ネットワーク ノード インターフェイス [2-386](#)

は

バースト バイト、QoS ポリサー [2-368, 2-373](#)
 ハードウェア ACL 統計情報 [2-461](#)
 パケットの転送、ACL の一致 [2-5](#)
 パケットのドロップ、ACL の一致 [2-5](#)
 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 [2-441](#)
 バックアップ、インターフェイス
 設定 [2-763](#)
 表示 [2-531](#)
 バンドル特性、UNI [2-160](#)

ひ

非 IP トラフィック アクセス リスト [2-304](#)
 非 IP トラフィックの転送
 許可 [2-364](#)
 拒否 [2-124](#)
 非 IP プロトコル
 拒否 [2-124](#)
 転送 [2-364](#)
 標準範囲 VLAN [2-818](#)

ふ

ファイル、削除 [2-116](#)

ブート ロードー

アクセス [A-1](#)

環境変数

設定 [A-21](#)

設定の表示 [A-21](#)

説明 [A-21](#)

場所 [A-23](#)

リセット [A-25](#)

起動

Cisco IOS イメージ [A-3](#)

ヘルパー イメージ [2-60](#)

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-8](#)

表示

使用可能なコマンド [A-13](#)

バージョン [A-27](#)

メモリ ヒープ使用率 [A-14](#)

ファイル

コピー [A-6](#)

削除 [A-7](#)

内容の表示 [A-5, A-16, A-24](#)

名前変更 [A-17](#)

リストの表示 [A-8](#)

ファイル システム

一貫性チェックの実行 [A-12](#)

フォーマット [A-11](#)

フラッシュの初期化 [A-10](#)

プロンプト [A-1](#)

負荷分散方式、EtherChannel [2-384](#)

物理ポート ラーナー [2-353](#)

不明なマルチキャスト トラフィック、回避 [2-767](#)

不明なユニキャスト トラフィック、回避 [2-767](#)

プライオリティ キューイング、QoS [2-396](#)

プライベート VLAN

アソシエーション [2-782](#)

混合ポート [2-773](#)

設定 [2-399](#)

表示 [2-678](#)

ポートの設定 [2-773](#)

ホスト ポート [2-773](#)

マッピング

設定 [2-782](#)

表示 [2-531](#)

プライマリ温度アラーム [2-11](#)

フレーム チェック シーケンス

「FCS」を参照

フレーム転送情報の表示 [B-8](#)

ブロードキャスト ストーム制御 [2-756](#)

フロントエンド コントローラ カウントとステータス情報 [B-10](#)

へ

ヘルス モニタリング診断テスト [2-127](#)

ほ

ポート シェーピング [2-460](#)

ポート セキュリティ

イネーブル化 [2-776](#)

違反エラーの回復 [2-154](#)

エージング [2-780](#)

デバッグ メッセージ、表示 [3-80](#)

ポート タイプ、MVR [2-349](#)

ポート、デバッグ [3-78](#)

ポート範囲、定義 [2-83, 2-98, 2-114](#)

ポート ベース認証

802.1x のグローバルなイネーブル化 [2-144](#)

ポートベース認証

2つの連続する EAPOL-Start フレームの間隔 [2-147](#)

- AAA 方式のリスト [2-3](#)
- EAP-Request/Identity フレームを再送信するまでの時間 [2-147](#)
- IEEE 802.1x AAA アカウンティング方式 [2-1](#)
- IEEE 802.1x の準備テスト [2-145](#)
- インターフェイスの初期化 [2-137, 2-146](#)
- オーセンティケータとしての PAE [2-141](#)
- 再認証の試行間隔 [2-147](#)
- スイッチからクライアントへの再送信時間 [2-147](#)
- スイッチから認証サーバへの再送信時間 [2-147](#)
- スイッチとクライアント間のフレーム再送信回数 [2-138 ~ 2-140](#)
- 設定可能な 802.1x パラメータのリセット [2-135](#)
- デバッグ メッセージ、表示 [3-3](#)
- 認証交換に失敗したあとの待機期間 [2-147](#)
- 認証サーバからクライアントへの応答時間 [2-147](#)
- 保留状態のサブリカント時間 [2-147](#)
- ポート、保護 [2-785](#)
- ホスト接続、ポート設定 [2-769](#)
- ホスト ポート、プライベート VLAN [2-773](#)
- ポリサー
 - CPU 保護用 [2-379](#)
 - 個別 [2-367](#)
 - 集約 [2-372, 2-377](#)
- ポリサーのデフォルト設定
 - NNI [B-29](#)
 - UNI [B-28](#)
- ポリシー マップ
 - QoS グループ ID の設定 [2-454](#)
 - インターフェイスへの適用 [2-382, 2-443, 2-456](#)
 - 親 [2-446](#)
 - および CoS 分類 [2-327](#)
 - および DSCP 分類 [2-328](#)
 - および IP precedence 分類 [2-330](#)
 - およびポリシング [2-370](#)
 - 階層 [2-445](#)
 - 子 [2-445](#)
 - 作成 [2-381](#)
 - 適用 [2-443](#)
 - トラフィックの分類、定義 [2-71](#)
 - トラフィック マーキング
 - CoS 値の設定 [2-448](#)
 - DSCP 値の設定 [2-450](#)
 - IP precedence 値の設定 [2-452](#)
 - 表示 [2-642](#)
 - プライオリティの設定 [2-396](#)
 - ポリサー
 - 単一クラス用 [2-367](#)
 - 複数のクラス [2-372, 2-377, 2-379, 2-445](#)
 - ポリシーマップ クラス コンフィギュレーション モード [2-71](#)
 - ポリシーマップ クラス、複数のアクションの設定 [2-96, 2-172, 2-815](#)
 - ポリシーマップ クラス ポリシング コンフィギュレーション モード [2-96, 2-370](#)
 - ポリシーマップ コンフィギュレーション モード [2-381](#)
 - ポリシング
 - クラスの複数の違反アクション [2-815](#)
 - クラスの複数の超過アクション [2-172](#)
 - クラスの複数の適合アクション [2-96](#)
 - プライオリティ [2-367](#)
 - ポリシング機能の設定
 - NNI のデフォルト [B-29](#)
 - UNI のデフォルト [B-28](#)
 - ポリシングを含むプライオリティ、QoS [2-396](#)

ま

- マクロ
 - global description の追加 [2-321](#)
 - インターフェイス範囲 [2-114, 2-181](#)
 - 作成 [2-322](#)
 - 説明の追加 [2-318](#)
 - 追跡 [2-319](#)
 - 適用 [2-319](#)
 - パラメータ値の指定 [2-319](#)
 - 表示 [2-636](#)
 - マッピング テーブル、QoS [2-795](#)

マップ

VLAN

- 作成 [2-822](#)
- 定義 [2-324](#)
- 表示 [2-683](#)

クラス

- 作成 [2-73](#)

マルチキャスト グループ、MVR [2-347](#)

マルチキャスト グループ アドレス、MVR [2-349](#)

マルチキャスト ストーム制御 [2-756](#)

マルチキャスト ルータ 学習方式 [2-237](#)

マルチキャスト ルータ ポート、IPv6 [2-278](#)

マルチキャスト ルータ ポート、設定 [2-237](#)

む

無効な GBIC

- エラー回復タイマー [2-154](#)
- エラー検出 [2-152](#)

め

メカニズムの検出、原因 [2-152](#)

メンテナンス エンド ポイント [2-811](#)

も

モード、MVR [2-346](#)

モード、コマンド [1-1](#)

ゆ

ユーザ EXEC モード [1-2, 1-3](#)

ユーザ ネットワーク インターフェイス [2-386](#)

優先順位

- QoS トラフィック マーキング用 [2-452](#)
- ポリシー マップでの設定 [2-452](#)

ユニキャスト ストーム制御 [2-756](#)

ら

ライン コンフィギュレーション モード [1-2, 1-5](#)

り

リソース テンプレート、表示 [2-661](#)

リンク フラップ

- エラー回復タイマー [2-154](#)
- エラー検出 [2-152](#)

る

ルーテッド ポート

- IP アドレス [2-189](#)
- サポートされる数 [2-189](#)

ルート ガード、スパニング ツリー用 [2-715](#)

ループ ガード、スパニング ツリー用 [2-715, 2-720](#)

ループバック エラー

- 回復タイマー [2-154](#)
- 検出 [2-152](#)

れ

レイヤ 2 traceroute

- IP アドレス [2-802](#)
- MAC アドレス [2-799](#)

レイヤ 2 プロトコル トンネリング エラー回復 [2-284](#)

レイヤ 2 プロトコル トンネル

- エラー回復タイマー [2-154](#)
- エラー検出 [2-152](#)

レイヤ 2 プロトコル トンネル カウンタ [2-81](#)

レイヤ 2 プロトコル ポートの表示 [2-586](#)

レシーバ ポート、MVR [2-349](#)

ろ

論理インターフェイス [2-179](#)