



## **Cisco IE 2000 スイッチ コマンド リファレンス**

Cisco IOS Release 15.0(2)EA

2013 年 5 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/](http://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またはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://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. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号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、ネットワークトポロジ図、およびその他の図は、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および電話番号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 IE 2000 スイッチ コマンド リファレンス  
© 2013 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### はじめに xxi

対象読者 xxi

目的 xxi

表記法 xxi

show コマンド出力のフィルタリング xxii

関連資料 xxii

マニュアルの入手方法およびテクニカル サポート xxiii

---

## CHAPTER 1

### コマンドライン インターフェイスの使用 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 IE 2000 スイッチ Cisco IOS コマンド 2-1

aaa accounting dot1x 2-1

aaa authentication dot1x 2-3

aaa authorization network 2-5

action 2-6

alarm contact 2-8

alarm facility fcs-hysteresis 2-10

alarm facility input-alarm 2-11

alarm facility power-supply 2-12

alarm facility sd-card 2-14

alarm facility temperature 2-15

alarm profile (グローバル コンフィギュレーション) 2-17

alarm profile (インターフェイス コンフィギュレーション) 2-19

alarm relay-mode 2-21

archive download-sw 2-22

|  |      |
|--|------|
| archive tar                                | 2-25 |
| archive upload-sw                          | 2-28 |
| arp access-list                            | 2-30 |
| authentication command bounce-port ignore  | 2-32 |
| authentication command disable-port ignore | 2-33 |
| authentication control-direction           | 2-34 |
| authentication event                       | 2-36 |
| authentication fallback                    | 2-40 |
| authentication host-mode                   | 2-42 |
| authentication mac-move permit             | 2-44 |
| authentication open                        | 2-46 |
| authentication order                       | 2-48 |
| authentication periodic                    | 2-50 |
| authentication port-control                | 2-52 |
| authentication priority                    | 2-54 |
| authentication timer                       | 2-56 |
| authentication violation                   | 2-58 |
| auto qos voip                              | 2-60 |
| boot buffersize                            | 2-65 |
| boot config-file                           | 2-66 |
| boot enable-break                          | 2-67 |
| boot fast                                  | 2-68 |
| boot helper                                | 2-69 |
| boot helper-config-file                    | 2-70 |
| boot host                                  | 2-71 |
| boot manual                                | 2-72 |
| boot private-config-file                   | 2-73 |
| boot system                                | 2-74 |
| channel-group                              | 2-75 |
| channel-protocol                           | 2-79 |
| cip enable                                 | 2-80 |
| cip security                               | 2-81 |
| cisp enable                                | 2-82 |
| class                                      | 2-83 |
| class-map                                  | 2-85 |

|  |       |
|--|-------|
| clear dot1x                            | 2-87  |
| clear eap sessions                     | 2-88  |
| clear errdisable interface             | 2-89  |
| clear arp inspection log               | 2-90  |
| clear ip arp inspection statistics     | 2-91  |
| clear ip dhcp snooping                 | 2-92  |
| clear ipc                              | 2-94  |
| clear ipv6 dhcp conflict               | 2-95  |
| clear lacp                             | 2-96  |
| clear mac address-table                | 2-97  |
| clear mac address-table move update    | 2-98  |
| clear nmsp statistics                  | 2-99  |
| clear pagp                             | 2-100 |
| clear port-security                    | 2-101 |
| clear psp counter                      | 2-103 |
| clear rep counters                     | 2-104 |
| clear spanning-tree counters           | 2-105 |
| clear spanning-tree detected-protocols | 2-106 |
| clear vmmps statistics                 | 2-108 |
| clear vtp counters                     | 2-109 |
| cluster commander-address              | 2-110 |
| cluster discovery hop-count            | 2-112 |
| cluster enable                         | 2-113 |
| cluster holdtime                       | 2-114 |
| cluster member                         | 2-115 |
| cluster outside-interface              | 2-117 |
| cluster run                            | 2-118 |
| cluster standby-group                  | 2-119 |
| cluster timer                          | 2-121 |
| define interface-range                 | 2-122 |
| delete                                 | 2-124 |
| deny (ARP アクセス リスト コンフィギュレーション)        | 2-125 |
| deny (MAC アクセス リスト コンフィギュレーション)        | 2-127 |
| dot1x                                  | 2-130 |
| dot1x auth-fail max-attempts           | 2-132 |

|                                       |       |
|---------------------------------------|-------|
| dot1x auth-fail vlan                  | 2-134 |
| dot1x control-direction               | 2-136 |
| dot1x credentials (グローバル コンフィギュレーション) | 2-138 |
| dot1x critical (グローバル コンフィギュレーション)    | 2-139 |
| dot1x critical (インターフェイス コンフィギュレーション) | 2-141 |
| dot1x default                         | 2-143 |
| dot1x fallback                        | 2-144 |
| dot1x guest-vlan                      | 2-145 |
| dot1x host-mode                       | 2-147 |
| dot1x initialize                      | 2-149 |
| dot1x mac-auth-bypass                 | 2-150 |
| dot1x max-reauth-req                  | 2-152 |
| dot1x max-req                         | 2-153 |
| dot1x pae                             | 2-154 |
| dot1x port-control                    | 2-155 |
| dot1x re-authenticate                 | 2-157 |
| dot1x reauthentication                | 2-158 |
| dot1x test eapol-capable              | 2-159 |
| dot1x test timeout                    | 2-160 |
| dot1x timeout                         | 2-161 |
| dot1x violation-mode                  | 2-163 |
| duplex                                | 2-164 |
| errdisable detect cause               | 2-166 |
| errdisable detect cause small-frame   | 2-169 |
| errdisable recovery cause small-frame | 2-171 |
| errdisable recovery                   | 2-172 |
| exception crashinfo                   | 2-175 |
| fallback profile                      | 2-176 |
| fcs-threshold                         | 2-178 |
| fixup                                 | 2-179 |
| flowcontrol                           | 2-180 |
| inside from                           | 2-182 |
| interface port-channel                | 2-184 |
| interface range                       | 2-186 |
| ip access-group                       | 2-188 |

|  |       |
|--|-------|
| ip address   | 2-191 |
| ip admission   | 2-193 |
| ip admission name proxy http   | 2-194 |
| ip arp inspection filter vlan  | 2-196 |
| ip arp inspection limit  | 2-198 |
| ip arp inspection log-buffer   | 2-200 |
| ip arp inspection trust  | 2-202 |
| ip arp inspection validate   | 2-204 |
| ip arp inspection vlan   | 2-206 |
| ip arp inspection vlan logging   | 2-207 |
| ip dhcp snooping   | 2-209 |
| ip dhcp snooping binding   | 2-210 |
| ip dhcp snooping database  | 2-212 |
| ip dhcp snooping information option                                    | 2-214 |
| ip dhcp snooping information option allow-untrusted                    | 2-216 |
| ip dhcp snooping information option format remote-id                   | 2-218 |
| ip dhcp snooping limit rate  | 2-219 |
| ip dhcp snooping trust   | 2-220 |
| ip dhcp snooping verify  | 2-221 |
| ip dhcp snooping vlan  | 2-222 |
| ip dhcp snooping vlan information option format-type circuit-id string | 2-223 |
| ip igmp filter   | 2-225 |
| ip igmp max-groups   | 2-226 |
| ip igmp profile  | 2-228 |
| ip igmp snooping   | 2-230 |
| ip igmp snooping last-member-query-interval                            | 2-232 |
| ip igmp snooping querier   | 2-234 |
| ip igmp snooping report-suppression                                    | 2-236 |
| ip igmp snooping tcn   | 2-238 |
| ip igmp snooping tcn flood   | 2-240 |
| ip igmp snooping vlan immediate-leave                                  | 2-241 |
| ip igmp snooping vlan mrouter  | 2-242 |
| ip igmp snooping vlan static   | 2-244 |
| ip source binding  | 2-246 |
| ip ssh   | 2-248 |

|  |       |
|--|-------|
| ip sticky-arp (インターフェイス コンフィギュレーション)           | 2-249 |
| ip verify source                               | 2-251 |
| ipv6 address dhcp                              | 2-253 |
| ipv6 dhcp client request vendor                | 2-254 |
| ipv6 dhcp ping packets                         | 2-255 |
| ipv6 dhcp pool                                 | 2-257 |
| ipv6 dhcp server                               | 2-260 |
| ipv6 mld snooping                              | 2-262 |
| ipv6 mld snooping last-listener-query-count    | 2-264 |
| ipv6 mld snooping last-listener-query-interval | 2-266 |
| ipv6 mld snooping listener-message-suppression | 2-268 |
| ipv6 mld snooping robustness-variable          | 2-269 |
| ipv6 mld snooping tcn                          | 2-271 |
| ipv6 mld snooping vlan                         | 2-273 |
| I2nat  | 2-275 |
| I2nat instance                                 | 2-277 |
| lacp port-priority                             | 2-279 |
| lacp system-priority                           | 2-281 |
| link-diag error-rate                           | 2-283 |
| link state group                               | 2-284 |
| link state track                               | 2-286 |
| location (グローバル コンフィギュレーション)                   | 2-287 |
| location (インターフェイス コンフィギュレーション)                | 2-289 |
| logging event                                  | 2-291 |
| logging event power-inline-status              | 2-292 |
| logging file                                   | 2-293 |
| mab request format attribute 32                | 2-295 |
| mac access-group                               | 2-297 |
| mac access-list extended                       | 2-299 |
| mac address-table aging-time                   | 2-301 |
| mac address-table learning vlan                | 2-302 |
| mac address-table move update                  | 2-304 |
| mac address-table notification                 | 2-306 |
| mac address-table static                       | 2-308 |
| mac address-table static drop                  | 2-309 |

- macro apply 2-311
- macro description 2-314
- macro description 2-317
- macro global 2-320
- macro global description 2-323
- macro name 2-324
- match (アクセス マップ コンフィギュレーション) 2-326
- match (クラスマップ コンフィギュレーション) 2-328
- mdix auto 2-330
- media-type rj45 2-331
- mls qos 2-332
- mls qos aggregate-policer 2-334
- mls qos cos 2-336
- mls qos dscp-mutation 2-338
- mls qos map 2-340
- mls qos queue-set output buffers 2-344
- mls qos queue-set output threshold 2-346
- mls qos rewrite ip dscp 2-348
- mls qos srr-queue input bandwidth 2-350
- mls qos srr-queue input buffers 2-352
- mls qos srr-queue input cos-map 2-354
- mls qos srr-queue input dscp-map 2-356
- mls qos srr-queue input priority-queue 2-358
- mls qos srr-queue input threshold 2-360
- mls qos srr-queue output cos-map 2-362
- mls qos srr-queue output dscp-map 2-364
- mls qos trust 2-366
- mls qos vlan-based 2-368
- monitor session 2-369
- mvr (グローバル コンフィギュレーション) 2-374
- mvr (インターフェイス コンフィギュレーション) 2-377
- network-policy 2-380
- network-policy profile (グローバル コンフィギュレーション) 2-381
- network-policy profile (ネットワークポリシー コンフィギュレーション) 2-383
- nmsp 2-385

[nmsp attachment suppress](#) 2-386  
[outside from](#) 2-387  
[pagp learn-method](#) 2-389  
[pagp port-priority](#) 2-391  
[permit \(ARP アクセス リスト コンフィギュレーション\)](#) 2-393  
[permit \(config-l2nat コンフィギュレーション\)](#) 2-395  
[permit \(MAC アクセス リスト コンフィギュレーション\)](#) 2-397  
[police](#) 2-400  
[police aggregate](#) 2-402  
[policy-map](#) 2-404  
[port-channel load-balance](#) 2-407  
[power inline](#) 2-409  
[power inline consumption](#) 2-412  
[power inline wattage](#) 2-414  
[power-supply dual](#) 2-416  
[priority-queue](#) 2-417  
[profinet](#) 2-419  
[psp](#) 2-421  
[ptp \(グローバル コンフィギュレーション\)](#) 2-423  
[ptp \(インターフェイス コンフィギュレーション\)](#) 2-425  
[queue-set](#) 2-427  
[radius-server dead-criteria](#) 2-428  
[radius-server host](#) 2-430  
[rcommand](#) 2-432  
[remote-span](#) 2-434  
[renew ip dhcp snooping database](#) 2-436  
[rep admin vlan](#) 2-438  
[rep block port](#) 2-439  
[rep lsl-age-timer](#) 2-442  
[rep preempt delay](#) 2-444  
[rep preempt segment](#) 2-445  
[rep segment](#) 2-446  
[rep stcn](#) 2-449  
[reserved-only](#) 2-450  
[rmon collection stats](#) 2-451

|                                      |       |
|--------------------------------------|-------|
| sdm prefer                           | 2-452 |
| service password-recovery            | 2-455 |
| service-policy                       | 2-457 |
| set                                  | 2-460 |
| setup                                | 2-462 |
| setup express                        | 2-465 |
| show access-lists                    | 2-467 |
| show alarm description port          | 2-470 |
| show alarm profile                   | 2-471 |
| show alarm settings                  | 2-473 |
| show archive status                  | 2-474 |
| show arp access-list                 | 2-475 |
| show authentication                  | 2-476 |
| show auto qos                        | 2-480 |
| show boot                            | 2-484 |
| show boot buffersize                 | 2-486 |
| show cable-diagnostics tdr           | 2-487 |
| show cip                             | 2-489 |
| show cisp                            | 2-491 |
| show class-map                       | 2-492 |
| show cluster                         | 2-493 |
| show cluster candidates              | 2-495 |
| show cluster members                 | 2-497 |
| show controllers cpu-interface       | 2-499 |
| show controllers ethernet-controller | 2-501 |
| show controllers power inline        | 2-508 |
| show controllers tcam                | 2-510 |
| show controllers utilization         | 2-512 |
| show dot1x                           | 2-514 |
| show dtp                             | 2-518 |
| show eap                             | 2-520 |
| show env                             | 2-522 |
| show env alarm-contact               | 2-523 |
| show errdisable detect               | 2-524 |
| show errdisable flap-values          | 2-526 |

|                                  |       |
|----------------------------------|-------|
| show errdisable recovery         | 2-527 |
| show etherchannel                | 2-529 |
| show facility-alarm status       | 2-532 |
| show fallback profile            | 2-533 |
| show fcs-threshold               | 2-535 |
| show flowcontrol                 | 2-537 |
| show interfaces                  | 2-539 |
| show interfaces counters         | 2-545 |
| show interfaces rep              | 2-547 |
| show inventory                   | 2-549 |
| show ip arp inspection           | 2-550 |
| show ip dhcp snooping            | 2-554 |
| show ip dhcp snooping binding    | 2-555 |
| show ip dhcp snooping database   | 2-557 |
| show ip dhcp snooping statistics | 2-559 |
| show ip igmp profile             | 2-562 |
| show ip igmp snooping            | 2-563 |
| show ip igmp snooping groups     | 2-566 |
| show ip igmp snooping mrouter    | 2-568 |
| show ip igmp snooping querier    | 2-569 |
| show ip source binding           | 2-571 |
| show ip verify source            | 2-572 |
| show ipc                         | 2-574 |
| show ipv6 dhcp conflict          | 2-578 |
| show ipv6 mld snooping           | 2-579 |
| show ipv6 mld snooping address   | 2-581 |
| show ipv6 mld snooping mrouter   | 2-583 |
| show ipv6 mld snooping querier   | 2-585 |
| show ipv6 route updated          | 2-587 |
| show l2nat instance              | 2-589 |
| show l2nat interface             | 2-590 |
| show l2nat statistics            | 2-592 |
| show l2nat statistics interface  | 2-595 |
| show lacp                        | 2-597 |
| show link-diag error-rate        | 2-601 |

|                                     |       |
|-------------------------------------|-------|
| show location                       | 2-602 |
| show link state group               | 2-604 |
| show mac access-group               | 2-606 |
| show mac address-table              | 2-607 |
| show mac address-table address      | 2-609 |
| show mac address-table aging-time   | 2-611 |
| show mac address-table count        | 2-613 |
| show mac address-table dynamic      | 2-615 |
| show mac address-table interface    | 2-617 |
| show mac address-table learning     | 2-619 |
| show mac address-table move update  | 2-620 |
| show mac address-table notification | 2-621 |
| show mac address-table static       | 2-623 |
| show mac address-table vlan         | 2-625 |
| show mls qos                        | 2-627 |
| show mls qos aggregate-policer      | 2-628 |
| show mls qos input-queue            | 2-629 |
| show mls qos interface              | 2-631 |
| show mls qos maps                   | 2-635 |
| show mls qos queue-set              | 2-638 |
| show mls qos vlan                   | 2-640 |
| show monitor                        | 2-641 |
| show mvr                            | 2-643 |
| show mvr interface                  | 2-645 |
| show mvr members                    | 2-647 |
| show network-policy profile         | 2-649 |
| show nmsp                           | 2-650 |
| show pagp                           | 2-653 |
| show parser macro                   | 2-655 |
| show policy-map                     | 2-658 |
| show port-security                  | 2-659 |
| show power inline                   | 2-661 |
| show profinet                       | 2-663 |
| show psp config                     | 2-665 |
| show psp statistics                 | 2-666 |

show ptp 2-667

show ptp port 2-670

show rep topology 2-671

show sdm prefer 2-674

show setup express 2-676

show spanning-tree 2-677

show storm-control 2-683

show system mtu 2-685

show udd 2-686

show version 2-689

show vlan 2-691

show vlan access-map 2-695

show vlan filter 2-696

show vmps 2-697

show vtp 2-699

shutdown 2-704

shutdown vlan 2-705

small-frame violation rate 2-706

snmp-server enable traps 2-708

snmp-server host 2-713

snmp trap mac-notification change 2-716

spanning-tree backbonefast 2-718

spanning-tree bpdupfilter 2-719

spanning-tree bpduguard 2-721

spanning-tree cost 2-723

spanning-tree etherchannel guard misconfig 2-725

spanning-tree extend system-id 2-726

spanning-tree guard 2-727

spanning-tree link-type 2-729

spanning-tree loopguard default 2-731

spanning-tree mode 2-733

spanning-tree mst configuration 2-734

spanning-tree mst cost 2-736

spanning-tree mst forward-time 2-738

spanning-tree mst hello-time 2-739

|   |       |
|---|-------|
| spanning-tree mst max-age                     | 2-740 |
| spanning-tree mst max-hops                    | 2-741 |
| spanning-tree mst port-priority               | 2-742 |
| spanning-tree mst pre-standard                | 2-744 |
| spanning-tree mst priority                    | 2-745 |
| spanning-tree mst root                        | 2-746 |
| spanning-tree port-priority                   | 2-748 |
| spanning-tree portfast (グローバル コンフィギュレーション)    | 2-750 |
| spanning-tree portfast (インターフェイス コンフィギュレーション) | 2-753 |
| spanning-tree transmit hold-count             | 2-755 |
| spanning-tree uplinkfast                      | 2-756 |
| spanning-tree vlan                            | 2-758 |
| speed   | 2-761 |
| srr-queue bandwidth limit                     | 2-763 |
| srr-queue bandwidth shape                     | 2-765 |
| srr-queue bandwidth share                     | 2-767 |
| storm-control                                 | 2-769 |
| switchport access                             | 2-772 |
| switchport autostate exclude                  | 2-774 |
| switchport backup interface                   | 2-776 |
| switchport block                              | 2-780 |
| switchport host                               | 2-781 |
| switchport mode                               | 2-782 |
| switchport nonegotiate                        | 2-785 |
| switchport port-security                      | 2-787 |
| switchport port-security aging                | 2-792 |
| switchport priority extend                    | 2-794 |
| switchport protected                          | 2-796 |
| switchport trunk                              | 2-797 |
| switchport voice vlan                         | 2-800 |
| sync flash sdfsflash                          | 2-802 |
| system mtu                                    | 2-803 |
| test cable-diagnostics tdr                    | 2-805 |
| test relay                                    | 2-806 |
| traceroute mac                                | 2-807 |

|                                     |       |
|-------------------------------------|-------|
| traceroute mac ip                   | 2-810 |
| trust                               | 2-812 |
| udld                                | 2-814 |
| udld port                           | 2-816 |
| udld reset                          | 2-818 |
| vlan                                | 2-819 |
| vlan access-map                     | 2-825 |
| vlan filter                         | 2-827 |
| vmmps reconfirm (特権 EXEC)           | 2-829 |
| vmmps reconfirm (グローバル コンフィギュレーション) | 2-830 |
| vmmps retry                         | 2-831 |
| vmmps server                        | 2-832 |
| vtp (グローバル コンフィギュレーション)             | 2-834 |
| vtp (インターフェイス コンフィギュレーション)          | 2-839 |
| vtp primary                         | 2-840 |

APPENDIX A

IE 2000 スイッチのブートローダ コマンド A-1

|            |      |
|------------|------|
| boot       | A-2  |
| cat        | A-4  |
| 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 |
| set        | A-20 |
| type       | A-23 |
| unset      | A-25 |
| version    | A-27 |

**APPENDIX B****IE 2000 スイッチ デバッグ コマンド B-1**

|                                 |      |
|---------------------------------|------|
| debug authentication            | B-2  |
| debug auto qos                  | B-4  |
| debug backup                    | B-6  |
| debug cip                       | B-7  |
| debug cisp                      | B-8  |
| debug cluster                   | B-9  |
| debug dot1x                     | B-11 |
| debug dtp                       | B-12 |
| debug eap                       | B-13 |
| debug etherchannel              | B-14 |
| debug interface                 | B-15 |
| debug ip dhcp snooping          | B-16 |
| debug ip verify source packet   | B-17 |
| debug ip igmp filter            | B-18 |
| debug ip igmp max-groups        | B-19 |
| debug ip igmp snooping          | B-20 |
| debug l2nat                     | B-21 |
| debug lacp                      | B-22 |
| debug lldp packets              | B-23 |
| debug mac-notification          | B-24 |
| debug matm                      | B-25 |
| debug matm move update          | B-26 |
| debug monitor                   | B-27 |
| debug mvrdbg                    | B-29 |
| debug nmsp                      | B-30 |
| debug nvram                     | B-31 |
| debug pagp                      | B-32 |
| debug platform acl              | B-33 |
| debug platform backup interface | B-35 |
| debug platform cisp             | B-36 |
| debug platform cpu-queues       | B-37 |
| debug platform dot1x            | B-39 |
| debug platform etherchannel     | B-40 |
| debug platform forw-tcam        | B-41 |

debug platform ip arp inspection B-42

debug platform ip dhcp B-43

debug platform ip igmp snooping B-44

debug platform ip source-guard B-46

debug platform ip unicast B-47

debug platform led B-49

debug platform matm B-50

debug platform messaging application B-51

debug platform phy B-52

debug platform pm B-54

debug platform port-asic B-56

debug platform port-security B-57

debug platform qos-acl-tcam B-58

debug platform resource-manager B-59

debug platform snmp B-60

debug platform span B-61

debug platform supervisor-asic B-62

debug platform sw-bridge B-63

debug platform tcam B-64

debug platform uuld B-67

debug platform vlan B-68

debug pm B-69

debug port-security B-71

debug profinet alarm B-72

debug profinet cyclic B-74

debug profinet error B-76

debug profinet packet B-78

debug profinet platform B-80

debug profinet topology B-82

debug profinet trace B-84

debug ptp B-86

debug qos-manager B-87

debug spanning-tree B-88

debug spanning-tree backbonefast B-90

debug spanning-tree bpdu B-91

|                                |       |
|--------------------------------|-------|
| debug spanning-tree bpdu-opt   | B-92  |
| debug spanning-tree mstp       | B-93  |
| debug spanning-tree switch     | B-95  |
| debug spanning-tree uplinkfast | B-97  |
| debug sw-vlan                  | B-98  |
| debug sw-vlan ifs              | B-100 |
| debug sw-vlan notification     | B-101 |
| debug sw-vlan vtp              | B-102 |
| debug udld                     | B-104 |
| debug vqpc                     | B-106 |

**APPENDIX C****Cisco IE 2000 スイッチ show platform コマンド C-1**

|   |      |
|---|------|
| show platform acl                       | C-2  |
| show platform backup interface          | C-3  |
| show platform configuration             | C-4  |
| show platform etherchannel              | C-5  |
| show platform forward                   | C-6  |
| show platform ip igmp snooping          | C-8  |
| show platform ip unicast                | C-9  |
| show platform ip unicast vrf compaction | C-11 |
| show platform ip unicast vrf tcam-label | C-12 |
| show platform ip wccp                   | C-13 |
| show platform ipv6 unicast              | C-14 |
| show platform layer4op                  | C-16 |
| show platform mac-address-table         | C-17 |
| show platform messaging                 | C-18 |
| show platform monitor                   | C-19 |
| show platform mvr table                 | C-20 |
| show platform pm                        | C-21 |
| show platform port-asic                 | C-22 |
| show platform port-security             | C-26 |
| show platform qos                       | C-27 |
| show platform resource-manager          | C-28 |
| show platform sdfsflash                 | C-30 |
| show platform snmp counters             | C-31 |
| show platform spanning-tree             | C-32 |

[show platform stp-instance](#) C-33

[show platform tcam](#) C-34

[show platform vlan](#) C-36

---

**APPENDIX D**

[オープン ソース ソフトウェアについて](#) D-1

---

**INDEX**



## はじめに

---

### 対象読者

このマニュアルは、Cisco IOS コマンドライン インターフェイス (CLI) を使って Cisco IE 2000 スイッチ (以降、スイッチ) を管理するネットワークング専門家を対象としています。このマニュアルは、すでに Cisco IOS コマンドおよびスイッチ ソフトウェア機能使用経験があることを前提としています。また、イーサネットと LAN のコンセプトおよび用語に関してすでに習得済みであることも前提としています。

### 目的

Cisco IE 2000 スイッチは LAN Base イメージまたは LAN Lite イメージのいずれかでサポートされます。LAN Base イメージでは、アクセス コントロール リスト (ACL) や Quality of Service (QoS) 機能といったインテリジェントなレイヤ 2 サービスが提供されます。IP サービス イメージには、レイヤ 2+ 機能およびレイヤ 3 ルーティング機能が含まれています。

このマニュアルでは、IE 2000 スイッチでの使用のために作成または変更されたレイヤ 2 コマンドおよびレイヤ 3 のコマンドに関する必要な情報を掲載しています。標準 Cisco IOS Release 15.0 コマンドについては、Cisco.com のホームページにアクセスして ([Technical Support & Documentation] > [Cisco IOS Software])、Cisco IOS のマニュアルセットを参照してください。

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

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

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

### 表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

- コマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。
- 角カッコ ([ ]) の中の要素は、省略可能です。

- 必ずどれか 1 つを選択しなければならない要素は、波カッコ ({} ) で囲み、縦棒 (|) で区切って示しています。
- 任意で選択する要素の中で、必ずどれか 1 つを選択しなければならない要素は、角カッコと波カッコで囲み、縦棒で区切って ({{|}}) 示しています。

対話形式の例では、次の表記法を使用しています。

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

(注)、注意、および警告には、次の表記法および記号を使用しています。



(注)

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



注意

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

## show コマンド出力のフィルタリング

**show** コマンドには、コマンド出力をフィルタするためのオプションの出力修飾子があります。

- | **begin** : *expression* と一致する行から表示を開始します。
- | **exclude** : *expression* と一致する行を表示から除外します。
- | **include** : *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。

文字列では、大文字と小文字が区別されます。| **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。

## 関連資料

次に挙げる、スイッチに関する詳細情報が記載されているマニュアルは、次の Cisco.com サイトから入手できます。

[http://www.cisco.com/en/US/products/ps9703/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9703/tsd_products_support_series_home.html)



(注)

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

- 初期設定情報については、スタートアップガイドの「Using Express Setup」またはハードウェア インストールガイドの付録「Configuring the Switch with the CLI-Based Setup Program」を参照してください。
- デバイスマネージャの要件については、リリースノート（発注できませんが、Cisco.com で入手可能）の「System Requirements」を参照してください。
- Network Assistant の要件については、『Getting Started with Cisco Network Assistant』（発注できませんが、Cisco.com で入手可能）を参照してください。

- クラスタの要件については、『*Release Notes for Cisco Network Assistant*』（発注できませんが、Cisco.com で入手可能）を参照してください。
- アップグレード情報については、リリース ノートの「**Downloading Software**」を参照してください。

スイッチに関するその他の情報については、次のマニュアルを参照してください。

- 『*Release Notes for the Cisco IE 2000 Switch*』
- 『*Cisco IE 2000 Switch Software Configuration Guide*』
- 『*Cisco IE 2000 スイッチ コマンド リファレンス*』
- 『*Cisco IE 2000 Switch System Message Guide*』
- 『*Cisco IE 2000 Switch Hardware Installation Guide*』
- 『*Cisco IE 2000 Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Cisco IE 2000 Switch*』
- Network Admission Control (NAC) 機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- これらの互換性マトリクス ドキュメントは、Cisco.com の次のページで入手可能です。

[http://www.cisco.com/en/US/products/hw/modules/ps5455/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html)

## 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* (マニュアルの変更内容)』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

## コマンドライン インターフェイスの使用

Cisco IE 2000 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 コマンドライン インターフェイス (CLI) の使用方法について説明します。

- これらの機能をサポートするコマンドの詳細な説明については、第 2 章「Cisco IE 2000 スイッチ Cisco IOS コマンド」を参照してください。
- ブートローダ コマンドの詳細については、付録 A「IE 2000 スイッチのブートローダ コマンド」を参照してください。
- **debug** コマンドの詳細については、付録 B「IE 2000 スイッチ デバッグ コマンド」を参照してください。
- **show platform** コマンドの詳細については、付録 C「Cisco IE 2000 スイッチ show platform コマンド」を参照してください。
- Cisco IOS Release 15.0 のさらに詳しい情報については、『Cisco IOS Release 15.0 Command Summary』を参照してください。
- タスク指向の設定手順については、このリリースのソフトウェア コンフィギュレーション ガイドを参照してください。

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

## 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
- config-vlan
- 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。<br>(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>              | <b>logout</b> コマンドを入力します。<br>特権 EXEC モードを開始するには、 <b>enable</b> コマンドを入力します。  |
| 特権 EXEC              | ユーザ EXEC モードから、 <b>enable</b> コマンドを入力します。   | Switch#              | ユーザ EXEC モードに戻る場合は、 <b>disable</b> コマンドを入力します。<br>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、 <b>configure</b> 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、 <b>configure</b> コマンドを入力します。   | Switch(config)#      | 特権 EXEC モードに戻る場合は、 <b>exit</b> または <b>end</b> コマンドを入力するか、 <b>Ctrl+Z</b> を押します。<br>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、 <b>interface</b> 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、 <b>interface</b> 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、 <b>end</b> コマンドを入力するか、 <b>Ctrl+Z</b> を押します。<br>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、 <b>exit</b> 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 <b>vlan vlan-id</b> 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、 <b>exit</b> コマンドを入力します。<br>特権 EXEC モードに戻る場合は、 <b>end</b> コマンドを入力するか、 <b>Ctrl+Z</b> 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、 <b>line</b> 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、 <b>exit</b> コマンドを入力します。<br>特権 EXEC モードに戻る場合は、 <b>end</b> コマンドを入力するか、 <b>Ctrl+Z</b> を押します。                                      |

## ユーザ EXEC モード

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

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

```
Switch> ?
```

## 特権 EXEC モード

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

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

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

```
Switch#
```

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

```
Switch> enable  
Switch#
```

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

```
Switch# ?
```

ユーザ EXEC モードに戻る場合は、**disable** 特権 EXEC コマンドを入力します。

## グローバル コンフィギュレーション モード

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

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

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

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

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

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

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

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

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

## インターフェイス コンフィギュレーション モード

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

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

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

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

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

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

## VLAN コンフィギュレーション モード

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

**config-vlan** モードを開始するには、**vlan vlan-id** グローバル コンフィギュレーション コマンドを入力します。

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

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

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

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

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

## ライン コンフィギュレーション モード

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

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

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

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

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

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





## CHAPTER 2

# Cisco IE 2000 スイッチ Cisco IOS コマンド

## aaa accounting dot1x

認証、許可、アカウントिंग (AAA) のアカウントングをイネーブルにし、回線単位またはインターフェイス単位で IEEE 802.1x セッションに対する特定のアカウントング方式を定義する方式リストを作成するには、グローバル コンフィギュレーション モードで **aaa accounting dot1x** 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

|                   |  |
|-------------------|--|
| <b>name</b>       | サーバ グループに名前を付けます。これは、 <b>broadcast group</b> および <b>group</b> 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。  |
| <b>default</b>    | デフォルト リストとして続くアカウントング方式を、アカウントング サービス用に指定します。  |
| <b>start-stop</b> | プロセスの開始時に <b>start</b> アカウントング通知を送信し、プロセスの終了時に <b>stop</b> アカウントング通知を送信します。 <b>start</b> 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 <b>start</b> 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。  |
| <b>broadcast</b>  | 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。   |
| <b>group</b>      | 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"><li>• <b>name</b> : サーバ グループ名</li><li>• <b>radius</b> : 全 RADIUS ホストのリスト</li><li>• <b>tacacs+</b> : 全 TACACS+ ホストのリスト</li></ul> <b>broadcast group</b> および <b>group</b> キーワードの後に入力する場合、 <b>group</b> キーワードはオプションです。オプションの <b>group</b> キーワードより多くのキーワードを入力できます。 |

## aaa accounting dot1x

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

**コマンドデフォルト** 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

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン** このコマンドは、RADIUS サーバへのアクセスが必要です。  
 インターフェイスに IEEE 802.1x RADIUS アカウンティングを設定する前に、**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを入力することを推奨します。

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

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



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

| コマンド                               | 説明   |
|------------------------------------|--|
| <b>aaa authentication dot1x</b>    | 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。  |
| <b>aaa new-model</b>               | 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 Software Command Reference, Release 15.0』を参照してください。 |
| <b>dot1x reauthentication</b>      | 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。  |
| <b>dot1x timeout reauth-period</b> | 再認証の間隔 (秒) を設定します。   |

# aaa authentication dot1x

認証、許可、アカウントिंग (AAA) の方式を IEEE 802.1x 認証に準拠するポートで使用するよう指定するには、グローバル コンフィギュレーション モードで **aaa authentication dot1x** 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} word
```

```
no aaa authentication dot1x {default}
```

## 構文の説明

|                |   |
|----------------|---|
| <b>default</b> | 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指定します。      |
| <b>word</b>    | 認証用のすべての RADIUS サーバの認証リスト名。有効な名前の長さは 1 ～ 31 文字です。 |



(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。

## コマンド デフォルト

認証は実行されません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

**group radius** を指定した場合、**radius-server host** グローバル コンフィギュレーション コマンドを使用して RADIUS サーバを設定する必要があります。

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

## 例

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

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

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

## 関連コマンド

| コマンド                       | 説明  |
|----------------------------|---|
| <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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# aaa authorization network

ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可を、IEEE 802.1x AAA ユーザアクセスコントロールリスト (ACL) または VLAN 割り当てなどを使用するようにスイッチを設定するには、グローバル コンフィギュレーション モードで **aaa authorization network** コマンドを使用します。RADIUS ユーザ認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

**aaa authorization network default group radius**

**no aaa authorization network default**

## 構文の説明

|                             |  |
|-----------------------------|--|
| <b>default group radius</b> | デフォルトの認証リストとして、サーバグループ内のすべての RADIUS ホストのリストを指定します。 |
|-----------------------------|--|

## コマンド デフォルト

認証はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

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

## 例

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

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

# action

VLAN アクセスマップ エントリのアクションを設定するには、アクセスマップ コンフィギュレーション モードで **action** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
action {drop | forward}
```

```
no action
```

## 構文の説明

|                |                              |
|----------------|------------------------------|
| <b>drop</b>    | 指定した条件に一致する場合に、パケットをドロップします。 |
| <b>forward</b> | 指定した条件に一致する場合に、パケットを転送します。   |

## コマンド デフォルト

デフォルトのアクションは、パケットの転送です。

## コマンド モード

アクセス マップ コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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、一致条件にアクセス コントロール リスト (ACL) 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** 形式では使用しません。

## 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   |
|--|--|
| <code>access-list {deny   permit}</code> | 番号付き標準 ACL を設定します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。  |
| <code>ip access-list</code>              | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <code>mac access-list extended</code>    | 名前付き MAC アドレス アクセス リストを作成します。  |
| <code>match (クラスマップ コンフィギュレーション)</code>  | VLAN マップの一致条件を定義します。   |
| <code>show vlan access-map</code>        | スイッチで作成された VLAN アクセス マップを表示します。  |
| <code>vlan access-map</code>             | VLAN アクセス マップを作成します。   |

# alarm contact

システム アラーム接点を設定するには、グローバル コンフィギュレーション モードで **alarm contact** のコマンドを使用します。

```
alarm contact contact {description {line} | severity {major | minor | none} | trigger {closed | open} | all}
```

```
no alarm contact contact {description {line} | severity {major | minor | none} | trigger {closed | open} | all}
```

## 構文の説明

|                                |                                |
|--------------------------------|--------------------------------|
| <i>contact</i>                 | アラーム接点番号を指定します。範囲番号は 1 ~ 2 です。 |
| <b>description</b> <i>line</i> | アラームを説明する文字列を設定します。            |
| <b>severity</b>                | レポートされる重大度を設定します。              |
| <b>major</b>                   | アラームをメジャーな重大度に設定します。           |
| <b>minor</b>                   | アラームをマイナーな重大度に設定します。           |
| <b>none</b>                    | 重大度を設定しません。                    |
| <b>trigger</b>                 | アラーム トリガーを設定します。               |
| <b>closed</b>                  | アラーム接点を閉じます。                   |
| <b>open</b>                    | アラーム接点を開きます。                   |
| <b>all</b>                     | すべてのアラーム接点を設定します。              |

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 例

次に、アラーム接点を 1 に設定し、重大度をメジャーに設定する例を示します。

```
Switch(config)# alarm contact 1 severity major
```

次に、アラーム接点 1 の重大度を解除する例を示します。

```
Switch(config)# no alarm contact 1 severity major
```

次に、アラーム 1 のトリガーを closed に設定する例を示します。

```
Switch(config)# alarm contact 1 trigger closed
```

次に、アラーム 1 のトリガーの closed を解除する例を示します。

```
Switch(config)# no alarm contact 1 trigger closed
```

## 関連コマンド

| コマンド                                | 説明                     |
|-------------------------------------|------------------------|
| <a href="#">show alarm settings</a> | すべてのスイッチのアラーム設定を表示します。 |

# 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 レートから変動率として設定するには、FCS ビット エラー レートの変動は、グローバル コンフィギュレーション モードで、**alarm facility fcs-hysteresis** 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

|            |                               |   |
|------------|-------------------------------|---|
| 構文の説明      | <i>percentage</i>             | 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。   |
| コマンド デフォルト |                               | デフォルトのしきい値は 10% です。入力アラームは両方とも、 <b>notifies</b> と <b>Syslog</b> に関連付けられます。  |
| コマンド モード   |                               | グローバル コンフィギュレーション   |
| コマンド履歴     | リリース                          | 変更内容  |
|            | 15.0(1)EY                     | このコマンドが導入されました。   |
| 使用上のガイドライン |                               | <p>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。</p> <p>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。FCS エラー レートは <b>fcs-threshold</b> インターフェイス コンフィギュレーション コマンドを使用してポート単位で設定します。</p> <p>しきい値がデフォルト値ではない場合、<b>show running-config</b> 特権 EXEC コマンドの出力に表示されます。</p> |
| 例          |                               | <p>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。</p> <pre>Switch(config)# <b>alarm facility fcs-hysteresis 5</b></pre>  |
| 関連コマンド     | コマンド                          | 説明  |
|            | <a href="#">fcs-threshold</a> | インターフェイスの FCS エラー レートを設定します。  |

# alarm facility input-alarm

外部の接点アラームを設定するには、グローバル コンフィギュレーション モードで **alarm facility input-alarm** コマンドを使用します。外部の接点アラーム設定をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**alarm facility input-alarm** *number* {**notifies** | **relay major** | **syslog**}

**no** **alarm facility input-alarm** *number* {**notifies** | **relay major** | **syslog**}

## 構文の説明

|                    |                            |
|--------------------|----------------------------|
| <b>number</b>      | アラーム接点番号。有効な値は 1 または 2 です。 |
| <b>notifies</b>    | システムがサーバに通知を送信できるようにします。   |
| <b>relay major</b> | メジャー リレー設定をイネーブルにします。      |
| <b>syslog</b>      | システム ロガーをイネーブルにします。        |

## コマンド デフォルト

なし

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次に、サーバに送信された通知で入力アラームを 2 に設定する例を示します。

```
Switch(config)# alarm facility 2 notifies
```

## 関連コマンド

| コマンド                                | 説明                       |
|-------------------------------------|--------------------------|
| <a href="#">show alarm settings</a> | 環境アラーム設定およびオプションが表示されます。 |

# alarm facility power-supply

システムがデュアル電源モードで稼働している場合に、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、グローバル コンフィギュレーション モードで **alarm facility power-supply** 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 | minor} | syslog}**

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

## 構文の説明

|                    |                                |
|--------------------|--------------------------------|
| <b>disable</b>     | 電源アラームをディセーブルにします。             |
| <b>notifies</b>    | 電源アラーム トラップを SNMP サーバに送信します。   |
| <b>relay major</b> | アラームをメジャー リレー回路に送信します。         |
| <b>relay minor</b> | アラームをマイナー リレー回路に送信します。         |
| <b>syslog</b>      | 電源アラーム トラップを syslog サーバに送信します。 |

## コマンド 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。デフォルトでは、両方の入力アラームは出力アラーム「Major」にマッピングされます。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 つめ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

次に、電源モニタリング アラームをディセーブルにする例を示します。

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

次に、SNMP サーバに通知を送信するように電源モニタリング アラームを設定する例を示します。

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

次の例では、電源モニタリング アラームをメジャー 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 major
Switch(config)#
```

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  
Switch(config)#
```

次に、syslog サーバに送信するように電源モニタリング アラームを設定する例を示します。

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

#### 関連コマンド

| コマンド                                       | 説明  |
|--|---|
| <a href="#">ptp (インターフェイス コンフィギュレーション)</a> | スイッチをデュアル電源モードで動作するように設定します。                          |
| <a href="#">show alarm settings</a>        | 環境アラーム設定およびオプションが表示されます。                              |
| <a href="#">snmp-server enable traps</a>   | スイッチでさまざまなトラップ タイプ SNMP 通知をネットワーク管理システム (NMS) に送信します。 |

# alarm facility sd-card

SD カードを設定するには、グローバル コンフィギュレーション モードで **alarm facility sd-card** コマンドを使用します。SD カードをデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**alarm facility sd-card {notifies | relay major | syslog}**

**no alarm facility sd-card {notifies | relay major | syslog}**

## 構文の説明

|                    |                          |
|--------------------|--------------------------|
| <b>notifies</b>    | システムがサーバに通知を送信できるようにします。 |
| <b>relay major</b> | メジャー リレー設定をイネーブルにします。    |
| <b>syslog</b>      | システム ロガーをイネーブルにします。      |

## コマンドデフォルト

なし

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、SD カードが取り付けられた場合に、サーバに通知するように入力アラームを設定する方法を示します。

```
Switch(config)# alarm facility sd-card notifies
```

## 関連コマンド

| コマンド                                | 説明                       |
|-------------------------------------|--------------------------|
| <a href="#">show alarm settings</a> | 環境アラーム設定およびオプションが表示されます。 |

# 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、グローバル コンフィギュレーション モードで **alarm facility temperature** 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 | minor} | syslog}}

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

## 構文の説明

|                    |   |
|--------------------|---|
| <b>primary</b>     | プライマリ モニタのアラームの温度を設定します。  |
| <b>high</b>        | 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。 |
| <b>low</b>         | 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。 |
| <b>notifies</b>    | 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。                              |
| <b>relay major</b> | 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をメジャー リレー回路に送信します。                                       |
| <b>syslog</b>      | 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。                            |
| <b>secondary</b>   | セカンダリ モニタのアラームの温度を設定します。  |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

セカンダリ温度アラームを使用してプライマリ温度の高温しきい値 (203 °F (95 °C)) より低い高温アラームをトリガーできます。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   |
|--|--|
| <a href="#">show alarm settings</a>      | 環境アラーム設定およびオプションが表示されます。                             |
| <a href="#">snmp-server enable traps</a> | スイッチでさまざまなトラップタイプ SNMP 通知をネットワーク管理システム (NMS) 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、グローバル コンフィギュレーション モードで **alarm profile** 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

*name* アラームのプロファイル名です。

### コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

アラームプロファイル コンフィギュレーション モードでは、次のコマンドが使用できます。

- **alarm alarm-id** : 指定したアラームをイネーブルにします。
- **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、コマンドのデフォルト値を設定します。
- **notifies alarm-id** : アラームの通知がイネーブルになり、簡易ネットワーク管理プロトコル (SNMP) 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 の出力を表示します。

表 2-1 では、アラーム ID と対応するアラームの説明を示します。

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、プロファイルを実験に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   |
|---|--|
| <b>alarm profile</b> (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。   |
| <b>show alarm settings</b>                  | 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。 |
| <b>snmp-server enable traps</b>             | スイッチでさまざまなトラップ タイプ SNMP 通知をネットワーク管理システム (NMS) 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接続するには、インターフェイス コンフィギュレーション モードで **alarm profile** 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。 |
|-------------|-----------------|

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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、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   |
|--|--|
| <b>alarm profile</b> (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。                     |
| <b>show alarm settings</b>               | 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 **alarm relay-mode** 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 energized**

**no alarm relay-mode energized**

|            |  |  |
|------------|--|--|
| 構文の説明      | <b>energized</b>                         | アラーム リレー モードを通電に設定します。   |
| コマンド デフォルト |  | アラーム リレーを通電解除します。  |
| 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     | <b>リリース</b>                              | <b>変更内容</b>  |
|            | 15.0(1)EY                                | このコマンドが導入されました。  |
| 使用上のガイドライン |  | アラーム リレーがにオープンされると、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。 |
| 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。<br>Switch(config)# <b>alarm relay-mode energized</b><br>Switch(config)#  |
| 関連コマンド     | <b>コマンド</b>                              | <b>説明</b>  |
|            | <b>alarm profile</b> (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。   |
|            | <b>show alarm profile</b>                | 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。                                   |
|            | <b>show alarm settings</b>               | 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

TFTP サーバから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持するには、特権 EXEC モードで **archive download-sw** コマンドを使用します。

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

## 構文の説明

|                          |  |
|--------------------------|--|
| <b>/directory</b>        | イメージのディレクトリを指定します。   |
| <b>/force-reload</b>     | 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。  |
| <b>/imageonly</b>        | 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。   |
| <b>/leave-old-sw</b>     | 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。   |
| <b>/no-set-boot</b>      | 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、BOOT 環境変数の設定は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。  |
| <b>/no-version-check</b> | スイッチ上で動作中のイメージとそのバージョンの互換性を確認せずに、ソフトウェア イメージをダウンロードします。  |
| <b>/overwrite</b>        | 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。   |
| <b>/reload</b>           | 設定が変更されて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。  |
| <b>/safe</b>             | 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。  |
| <b>source-url</b>        | 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"> <li>ローカル フラッシュ ファイル システムの構文<br/><b>flash:</b></li> <li>FTP の構文 :<br/><b>ftp:[[/username[:password]@location]/directory]/image-name.tar</b></li> <li>HTTP サーバの構文 :<br/><b>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>セキュア HTTPS サーバの構文 :<br/><b>https://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>Remote Copy Protocol (RCP) の構文 :<br/><b>rcp:[[/username@location]/directory]/image-name.tar</b></li> <li>TFTP の構文 :<br/><b>tftp:[[/location]/directory]/image-name.tar</b></li> </ul> <b>image-name.tar</b> 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。 |

**コマンド デフォルト**

現行のソフトウェア イメージは、ダウンロードされたイメージで上書きされません。  
ソフトウェア イメージと HTML ファイルの両方がダウンロードされます。  
新しいイメージは **flash:** ファイル システムにダウンロードされます。  
BOOT 環境変数は、**flash:** ファイル システムの新しいソフトウェア イメージを示すよう変更されます。  
イメージ名では大文字と小文字が区別されます。イメージ ファイルは **tar** フォーマットで提供されま  
す。

**コマンド モード**

特権 EXEC

**コマンド履歴**

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン**

一度に 1 つずつのディレクトリを指定するには、**archive download-sw /directory** コマンドを使用しま  
す。

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

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

**/leave-old-sw** オプションを使用し、新しいイメージをダウンロードしたときに古いイメージが上書き  
されなかった場合、**delete** 特権 EXEC コマンドを使用して古いイメージを削除することができます。  
詳細については、「**delete**」(P.2-124) を参照してください。

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。

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

**例**

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

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

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

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

## ■ archive download-sw

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   |
|-----------------------------------|--|
| <a href="#">archive tar</a>       | 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。 |
| <a href="#">archive upload-sw</a> | 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。                            |
| <a href="#">delete</a>            | 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

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うには、特権 EXEC モードで **archive tar** コマンドを使用します。

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

## 構文の説明

**/create destination-url**  
**flash:/file-url**

ローカルまたはネットワーク ファイル システムに新しい tar ファイルを作成します。

*destination-url* には、ローカルまたはネットワーク ファイル システムの宛先 URL エイリアス、および作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの構文  
**flash:**
- FTP の構文 :  
**ftp:[[/username[:password]@location]/directory]/tar-filename.tar**
- HTTP サーバの構文 :  
**http://[[username:password]@]{hostname | host-ip}/[directory]/image-name.tar**
- セキュア HTTPS サーバの構文 :  
**https://[[username:password]@]{hostname | host-ip}/[directory]/image-name.tar**
- Remote Copy Protocol (RCP) の構文 :  
**rnp:[[/username@location]/directory]/tar-filename.tar**
- TFTP の構文 : **tftp:[[/location]/directory]/tar-filename.tar**

*tar-filename.tar* は、作成する tar ファイルです。

**flash:/file-url** には、新しい tar ファイルの作成元になる、ローカル フラッシュ ファイル システム上の場所を指定します。

送信元ディレクトリ内のファイルまたはディレクトリのオプションのリストを指定して、新しい tar ファイルに書き込むことができます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

|   |   |
|---|---|
| <b>/table source-url</b>                                    | <p>既存の tar ファイルの内容を画面に表示します。</p> <p><i>source-url</i> 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"> <li>ローカル フラッシュ ファイル システムの構文<br/><b>flash:</b></li> <li>FTP の構文 :<br/><b>ftp:[[/username[:password]@]location]/directory]/tar-filename.tar</b></li> <li>HTTP サーバの構文 :<br/><b>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>セキュア HTTPS サーバの構文 :<br/><b>https://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>RCP の構文 :<br/><b>rpc:[/username@location]/directory]/tar-filename.tar</b></li> <li>TFTP の構文 : <b>tftp:[/location]/directory]/tar-filename.tar</b></li> </ul>  |
| <b>/xtract source-url<br/>flash:/file-url [dir/file...]</b> | <p><i>tar</i> 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 の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"> <li>ローカル フラッシュ ファイル システムの構文<br/><b>flash:</b></li> <li>FTP の構文 :<br/><b>ftp:[[/username[:password]@]location]/directory]/tar-filename.tar</b></li> <li>HTTP サーバの構文 :<br/><b>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>セキュア HTTPS サーバの構文 :<br/><b>https://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>RCP の構文 :<br/><b>rpc:[/username@location]/directory]/tar-filename.tar</b></li> <li>TFTP の構文 : <b>tftp:[/location]/directory]/tar-filename.tar</b></li> </ul> <p><i>tar-filename.tar</i> は、抽出される tar ファイルです。</p> <p><b>flash:/file-url [dir/file...]</b> 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> |

コマンド 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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

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:cies-lanbase-tar.12-44.EX.tar
info (219 bytes)
```

```
cies-lanbase-mz.12-44.EX/ (directory)
cies-lanbase-mz.12-44.EX (610856 bytes)
cies-lanbase-mz.12-44.EX/info (219 bytes)
info.ver (219 bytes)
```

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

```
flash:cies-lanbase-tar.12-44.EX.tar cies-lanbase-12-44.EX/html
cies-lanbase-mz.12-44.EX/html/ (directory)
cies-lanbase-mz.12-44.EX/html/const.htm (556 bytes)
cies-lanbase-mz.12-44.EX/html/xhome.htm (9373 bytes)
cies-lanbase-mz.12-44.EX/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                                |
|--------|-------------------------------------|-----------------------------------|
|        | <a href="#">archive download-sw</a> | 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。 |
|        | <a href="#">archive upload-sw</a>   | 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

スイッチの既存のイメージをサーバにアップロードするには、特権 EXEC モードで **archive upload-sw** コマンドを使用します。

**archive upload-sw** [/version *version\_string*] *destination-url*

## 構文の説明

|                                       |  |
|---------------------------------------|--|
| <b>/version</b> <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。  |
| <i>destination-url</i>                | 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"> <li>ローカル フラッシュ ファイル システムの構文<br/><b>flash:</b></li> <li>FTP の構文 :<br/><b>ftp:[[/username[:password]@]location]/directory/image-name.tar</b></li> <li>HTTP サーバの構文 :<br/><b>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>セキュア HTTPS サーバの構文 :<br/><b>https://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>Secure Copy Protocol (SCP) の構文 :<br/><b>scp:[[/username@]location]/directory/image-name.tar</b></li> <li>Remote Copy Protocol (RCP) の構文 :<br/><b>rnp:[[/username@]location]/directory/image-name.tar</b></li> <li>TFTP の構文 :<br/><b>tftp:[[/location]/directory]/image-name.tar</b></li> </ul> <p><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。</p> |

## コマンドデフォルト

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

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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   |
|-------------------------------------|--|
| <a href="#">archive download-sw</a> | 新しいイメージをスイッチにダウンロードします。                                |
| <a href="#">archive tar</a>         | 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

アドレス解決プロトコル (ARP) アクセス コントロール リスト (ACL) を定義する場合、または定義済みリストの末尾に句を追加する場合は、グローバル コンフィギュレーション モードで **arp access-list** コマンドを使用します。指定された ARP アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

**arp access-list** *acl-name*

**no arp access-list** *acl-name*

## 構文の説明

*acl-name* ACL の名前

## コマンドデフォルト

ARP アクセス リストは定義されていません。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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** : 拒否するパケットを指定します。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.2-125) 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** : 転送するパケットを指定します。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.-393) 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  |
|--|---|
| <b>deny</b> (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。    |
| <b>ip arp inspection filter vlan</b>     | 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。 |
| <b>permit</b> (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。    |
| <b>show arp access-list</b>              | ARP アクセス リストに関する詳細を表示します。                     |

# authentication command bounce-port ignore

スイッチ スタックまたはスタンドアロン スイッチ上で、ポートを一時的にディセーブルにするコマンドをスイッチが無視できるようにするには、グローバル コンフィギュレーション モードで **authentication command bounce-port ignore** コマンドを使用します。デフォルトのステータスに戻すには、このコマンドの **no** 形式を使用します。

**authentication command bounce-port ignore**

**no authentication command bounce-port ignore**



(注)

このコマンドを使用するには、スイッチが LAN Base イメージまたは IP Base イメージを実行している必要があります。

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

このスイッチは、RADIUS 認可変更 (CoA) **bounce port** コマンドを受け入れます。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

## 例

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

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

## 関連コマンド

| コマンド   | 説明   |
|--|--|
| <a href="#">authentication command disable-port ignore</a> | スイッチが CoA <b>disable port</b> コマンドを無視するように設定します。 |

# authentication command disable-port ignore

スイッチ スタックまたはスタンドアロン スイッチ上で、ポートをディセーブルにするコマンドをスイッチが無視できるようにするには、グローバル コンフィギュレーション モードで **authentication command disable-port ignore** コマンドを使用します。デフォルトのステータスに戻すには、このコマンドの **no** 形式を使用します。

**authentication command disable-port ignore**

**no authentication command disable-port ignore**



(注)

このコマンドを使用するには、スイッチが LAN Base イメージまたは IP Base イメージを実行している必要があります。

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

このスイッチは、RADIUS 認可変更 (CoA) **disable port** コマンドを受け入れます。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

## 例

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

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

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">authentication command bounce-port ignore</a> | スイッチが CoA <b>bounce port</b> コマンドを無視するように設定します。 |

# authentication control-direction

ポート制御を単方向または双方向に設定するには、インターフェイス コンフィギュレーション モードで **authentication control-direction** コマンドを使用します。デフォルト設定に戻すには、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

|             |   |
|-------------|---|
| <b>both</b> | 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。         |
| <b>in</b>   | ポートの単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。 |

## コマンド デフォルト

ポートは双方向モードに設定されています。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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   |
|---------------------------------|--|
| <b>authentication event</b>     | 特定の認証イベントのアクションを設定します。   |
| <b>authentication fallback</b>  | 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。 |
| <b>authentication host-mode</b> | ポートで認証マネージャ モードを設定します。   |
| <b>authentication open</b>      | 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。                                  |
| <b>authentication order</b>     | ポートで使用する認証方式の順序を設定します。   |
| <b>authentication periodic</b>  | 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  |
|------------------------------------|---|
| <b>authentication port-control</b> | 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。   |
| <b>authentication priority</b>     | ポート プライオリティ リストに認証方式を追加します。   |
| <b>authentication timer</b>        | 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。                                       |
| <b>authentication violation</b>    | 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。 |
| <b>show authentication</b>         | スイッチの認証マネージャ イベントに関する情報を表示します。  |

# authentication event

ポートの特定の認証イベントのアクションを設定するには、インターフェイス コンフィギュレーション モードで **authentication event** 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。

```
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

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

## コマンド デフォルト

イベント応答はポートに設定されません。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 を稼働し、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-Success メッセージを受信しても、DHCP 設定プロセスが再開しない場合があります。

*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。

リモートスイッチドポートアナライザ (RSPAN) *VLAN*、音声 *VLAN* 以外のアクティブなすべての *VLAN* は、IEEE 802.1x のゲスト *VLAN* として設定できます。ゲスト *VLAN* 機能は、アクセスポートでだけサポートされます。内部 *VLAN* (ルーテッドポート) またはトランクポートではサポートされません。

- MAC 認証バイパスが IEEE 802.1x ポートでイネーブルの場合に、EAPOL メッセージ交換を待機している間に IEEE802.1x 認証が期限切れになると、スイッチでは、クライアントの MAC アドレスに基づいてクライアントを許可できます。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネットパケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。
  - 認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。
  - 認証に失敗すると、スイッチはポートにゲスト *VLAN* を割り当てます (指定されていない場合)。

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

*authentication-fail* イベントの場合：

- サプリカントが認証に失敗すると、ポートは制限 *VLAN* に移動され、EAP 成功メッセージがサ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。

制限付き VLAN による再認証。再認証がディセーブルにされていると、制限 VLAN 内のポートは、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。マルチ認証 (multiauth) モードのポートの場合、またはポートの音声ドメインが MDA モードである場合、このコマンドを使用します。

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

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

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

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

**関連コマンド**

| コマンド                                    | 説明   |
|---|--|
| <b>authentication control-direction</b> | ポート モードを単一方向または双方向に設定します。  |
| <b>authentication fallback</b>          | 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。 |
| <b>authentication host-mode</b>         | ポートで認証マネージャ モードを設定します。   |
| <b>authentication open</b>              | 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  |
|------------------------------------|---|
| <b>authentication order</b>        | ポートで使用する認証方式の順序を設定します。  |
| <b>authentication periodic</b>     | 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。   |
| <b>authentication port-control</b> | 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。   |
| <b>authentication priority</b>     | ポート プライオリティ リストに認証方式を追加します。   |
| <b>authentication timer</b>        | 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。                                 |
| <b>authentication violation</b>    | 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。 |
| <b>show authentication</b>         | 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

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にポートを設定するには、インターフェイス コンフィギュレーション モードで **authentication fallback** コマンドを使用します。デフォルト設定に戻すには、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。

## コマンドデフォルト

フォールバックはイネーブルではありません。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                                |
|---|-----------------------------------|
| <b>authentication control-direction</b> | ポート モードを単一方向または双方向に設定します。         |
| <b>authentication event</b>             | 特定の認証イベントのアクションを設定します。            |
| <b>authentication host-mode</b>         | ポートで認証マネージャ モードを設定します。            |
| <b>authentication open</b>              | 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。 |
| <b>authentication order</b>             | ポートで使用する認証方式の順序を設定します。            |
| <b>authentication periodic</b>          | 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。       |
| <b>authentication port-control</b>      | 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  |
|---------------------------------|---|
| <b>authentication priority</b>  | ポートプライオリティ リストに認証方式を追加します。  |
| <b>authentication timer</b>     | 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。                               |
| <b>authentication violation</b> | 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。 |
| <b>show authentication</b>      | 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、インターフェイス コンフィギュレーション モードで **authentication host-mode** 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。

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

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

## 構文の説明

|                     |   |
|---------------------|---|
| <b>multi-auth</b>   | (任意) 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。 |
| <b>multi-domain</b> | (任意) ポートのマルチドメイン モードをイネーブルにします。               |
| <b>multi-host</b>   | (任意) ポートのマルチホスト モードをイネーブルにします。                |
| <b>single-host</b>  | (任意) ポートのシングルホスト モードをイネーブルにします。               |

## コマンド デフォルト

シングルホスト モードがイネーブルにされています。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

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

ハブの背後にデバイスを配置し、それぞれを認証してポート アクセスのセキュリティを確保できるようにするには、マルチ認証モードに設定する必要があります。音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは 1 つだけです。

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

## 例

次の例では、ポートのマルチ認証モードをイネーブルにする方法を示します。

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

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

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

次の例では、ポートのマルチホスト モードをイネーブルにする方法を示します。

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

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

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

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

#### 関連コマンド

| コマンド                                    | 説明  |
|---|---|
| <b>authentication control-direction</b> | ポート モードを単一方向または双方向に設定します。   |
| <b>authentication event</b>             | 特定の認証イベントのアクションを設定します。  |
| <b>authentication fallback</b>          | 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。        |
| <b>authentication open</b>              | 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。   |
| <b>authentication order</b>             | ポートで使用する認証方式の順序を設定します。  |
| <b>authentication periodic</b>          | 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。   |
| <b>authentication port-control</b>      | 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。   |
| <b>authentication priority</b>          | ポート プライオリティ リストに認証方式を追加します。   |
| <b>authentication timer</b>             | 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。                                 |
| <b>authentication violation</b>         | 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。 |
| <b>show authentication</b>              | 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

スイッチで MAC 移動をイネーブルにするには、グローバル コンフィギュレーション モードで **authentication mac-move permit** コマンドを使用します。デフォルト設定に戻すには、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。

## コマンドデフォルト

MAC 移動はイネーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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   |
|---------------------------------|--|
| <b>authentication event</b>     | 特定の認証イベントのアクションを設定します。   |
| <b>authentication fallback</b>  | 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。 |
| <b>authentication host-mode</b> | ポートで認証マネージャ モードを設定します。   |
| <b>authentication open</b>      | 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。                                  |
| <b>authentication order</b>     | ポートで使用する認証方式の順序を設定します。   |
| <b>authentication periodic</b>  | 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  |
|------------------------------------|---|
| <b>authentication port-control</b> | 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。   |
| <b>authentication priority</b>     | ポート プライオリティ リストに認証方式を追加します。   |
| <b>authentication timer</b>        | 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。                                       |
| <b>authentication violation</b>    | 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。 |
| <b>show authentication</b>         | 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

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するには、インターフェイス コンフィギュレーション モードで **authentication open** コマンドを使用します。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**

**コマンド デフォルト**      オープン アクセスはディセーブルにされています。

**コマンド モード**      インターフェイス コンフィギュレーション

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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   |
|--------|---|--|
|        | <b>authentication control-direction</b> | ポート モードを単一方向または双方向に設定します。  |
|        | <b>authentication event</b>             | 特定の認証イベントのアクションを設定します。   |
|        | <b>authentication fallback</b>          | 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。 |
|        | <b>authentication host-mode</b>         | ポートで認証マネージャ モードを設定します。   |
|        | <b>authentication order</b>             | ポートで使用する認証方式の順序を設定します。   |
|        | <b>authentication periodic</b>          | 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。  |
|        | <b>authentication port-control</b>      | 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。  |
|        | <b>authentication priority</b>          | 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  |
|---------------------------------|---|
| <b>authentication timer</b>     | 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。                               |
| <b>authentication violation</b> | 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。 |
| <b>show authentication</b>      | 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

ポートで使用する認証方式の順序を設定するには、インターフェイス コンフィギュレーション モードで **authentication order** 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。

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

```
no authentication order
```

## 構文の説明

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

## コマンドデフォルト

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

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                        |
|--|---------------------------|
| <a href="#">authentication control-direction</a> | ポート モードを単一方向または双方向に設定します。 |
| <a href="#">authentication event</a>             | 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  |
|------------------------------------|---|
| <b>authentication fallback</b>     | 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。        |
| <b>authentication host-mode</b>    | ポートで認証マネージャ モードを設定します。  |
| <b>authentication open</b>         | 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。   |
| <b>authentication periodic</b>     | 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。   |
| <b>authentication port-control</b> | ポートの認証ステートの手動制御をイネーブルにします。  |
| <b>authentication priority</b>     | ポート プライオリティ リストに認証方式を追加します。   |
| <b>authentication timer</b>        | 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。                               |
| <b>authentication violation</b>    | 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。 |
| <b>mab</b>                         | ポートの MAC 認証バイパスをイネーブルにします。  |
| <b>mab eap</b>                     | Extensible Authentication Protocol (EAP) を使用するようポートを設定します。                |
| <b>show authentication</b>         | 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

ポートで再認証をイネーブルまたはディセーブルにするには、インターフェイス コンフィギュレーション モードで **authentication periodic** コマンドを使用します。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**

## 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

再認証はディセーブルにされています。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

## 例

次の例では、ポートの定期的再認証をイネーブルにする方法を示します。

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

次の例では、ポートの定期的再認証をディセーブルにする方法を示します。

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

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

## 関連コマンド

| コマンド                                    | 説明   |
|---|--|
| <b>authentication control-direction</b> | ポート モードを単一方向または双方向に設定します。  |
| <b>authentication event</b>             | 特定の認証イベントのアクションを設定します。   |
| <b>authentication fallback</b>          | 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。 |
| <b>authentication host-mode</b>         | ポートで認証マネージャ モードを設定します。   |
| <b>authentication open</b>              | 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。                                  |
| <b>authentication order</b>             | ポートで使用する認証方式の順序を設定します。   |
| <b>authentication port-control</b>      | 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  |
|---------------------------------|---|
| <b>authentication priority</b>  | ポートプライオリティ リストに認証方式を追加します。  |
| <b>authentication timer</b>     | 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。                               |
| <b>authentication violation</b> | 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。 |
| <b>show authentication</b>      | 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

ポートの認証ステータスの手動制御をイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication port-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

## 構文の説明

|                            |   |
|----------------------------|---|
| <b>auto</b>                | 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。                  |
| <b>force-authorized</b>    | 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。 |
| <b>force-un authorized</b> | 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。                      |

## コマンドデフォルト

デフォルトの設定は **force-authorized** です。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。
- スイッチド ポート アナライザ (SPAN) および Remote SPAN (RSPAN) 宛先ポート：SPAN または RSPAN 宛先ポートであるポートの IEEE 802.1x 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先として削除されるまで、IEEE 802.1x 認証はディセーブルのままです。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

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

**例**

次の例では、ポート ステートを自動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  |
|---|---|
| <b>authentication control-direction</b> | ポート モードを単方向または双方向に設定します。  |
| <b>authentication event</b>             | 特定の認証イベントのアクションを設定します。  |
| <b>authentication fallback</b>          | 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。        |
| <b>authentication host-mode</b>         | ポートで認証マネージャ モードを設定します。  |
| <b>authentication open</b>              | 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。   |
| <b>authentication order</b>             | ポートで使用する認証方式の順序を設定します。  |
| <b>authentication periodic</b>          | 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。   |
| <b>authentication priority</b>          | ポート プライオリティ リストに認証方式を追加します。   |
| <b>authentication timer</b>             | 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。                                 |
| <b>authentication violation</b>         | 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。 |
| <b>show authentication</b>              | 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

ポート プライオリティ リストに認証方式を追加するには、インターフェイス コンフィギュレーション モードで **authentication priority** 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。

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

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

## 構文の説明

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

## コマンドデフォルト

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

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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  |
|---|---|
| <b>authentication control-direction</b> | ポート モードを単一方向または双方向に設定します。   |
| <b>authentication event</b>             | 特定の認証イベントのアクションを設定します。  |
| <b>authentication fallback</b>          | 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。        |
| <b>authentication host-mode</b>         | ポートで認証マネージャ モードを設定します。  |
| <b>authentication open</b>              | 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。   |
| <b>authentication order</b>             | ポートで使用する認証方式の順序を設定します。  |
| <b>authentication periodic</b>          | 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。   |
| <b>authentication port-control</b>      | 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。   |
| <b>authentication timer</b>             | 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。                                 |
| <b>authentication violation</b>         | 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。 |
| <b>mab</b>                              | ポートの MAC 認証バイパスをイネーブルにします。  |
| <b>mab eap</b>                          | Extensible Authentication Protocol (EAP) を使用するようポートを設定します。                |
| <b>show authentication</b>              | 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

802.1x 対応ポートのタイムアウトと再認証パラメータを設定するには、インターフェイス コンフィギュレーション モードで **authentication timer** 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。

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

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

## 構文の説明

|                       |   |
|-----------------------|---|
| <b>inactivity</b>     | (任意) 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を指定します。 |
| <b>reauthenticate</b> | (任意) 自動再認証の試行を開始するまでの時間を秒単位で指定します。                    |
| <b>server</b>         | (任意) 無許可ポートの認証の試行が行われるまでの間隔を秒単位で指定します。                |
| <b>restart</b>        | (任意) 無許可ポートの認証の試行が行われるまでの間隔を秒単位で指定します。                |
| <b>value</b>          | (任意) 1 から 65535 までの値 (秒) を入力します。                      |

## コマンドデフォルト

**inactivity**、**server**、および **restart** キーワードは 60 秒に設定されます。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                        |
|--|---------------------------|
| <a href="#">authentication control-direction</a> | ポート モードを単一方向または双方向に設定します。 |
| <a href="#">authentication event</a>             | 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  |
|------------------------------------|---|
| <b>authentication fallback</b>     | 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。        |
| <b>authentication host-mode</b>    | ポートで認証マネージャ モードを設定します。  |
| <b>authentication open</b>         | 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。   |
| <b>authentication order</b>        | ポートで使用する認証方式の順序を設定します。  |
| <b>authentication periodic</b>     | 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。   |
| <b>authentication port-control</b> | 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。   |
| <b>authentication priority</b>     | ポート プライオリティ リストに認証方式を追加します。   |
| <b>authentication violation</b>    | 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。 |
| <b>show authentication</b>         | 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

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するには、インターフェイス コンフィギュレーション モードで **authentication violation** 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。

```
authentication violation {protect | restrict | shutdown}
```

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

## 構文の説明

|                 |   |
|-----------------|---|
| <b>protect</b>  | 予期しない着信 MAC アドレスはドロップされます。syslog エラーは生成されません。       |
| <b>restrict</b> | 違反エラーの発生時に Syslog エラーを生成します。                        |
| <b>shutdown</b> | 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。 |

## コマンドデフォルト

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

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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
```

**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   |
|---|--|
| <b>authentication control-direction</b> | ポート モードを単一方向または双方向に設定します。  |
| <b>authentication event</b>             | 特定の認証イベントのアクションを設定します。   |
| <b>authentication fallback</b>          | 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。 |

| コマンド                               | 説明  |
|------------------------------------|---|
| <b>authentication host-mode</b>    | ポートで認証マネージャ モードを設定します。                    |
| <b>authentication open</b>         | 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。         |
| <b>authentication order</b>        | ポートで使用する認証方式の順序を設定します。                    |
| <b>authentication periodic</b>     | 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。               |
| <b>authentication port-control</b> | 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。               |
| <b>authentication priority</b>     | ポート プライオリティ リストに認証方式を追加します。               |
| <b>authentication timer</b>        | 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。 |
| <b>show authentication</b>         | スイッチの認証マネージャ イベントに関する情報を表示します。            |

# auto qos voip

QoS ドメイン内の Voice over IP (VoIP) の Quality of Service (QoS) を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos voip** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                        |  |
|------------------------|--|
| <b>cisco-phone</b>     | このポートが Cisco IP Phone に接続されていると判断し、自動的に VoIP の QoS を設定します。着信パケットの QoS ラベルが信頼されるのは、IP Phone が検知される場合に限りです。  |
| <b>cisco-softphone</b> | このポートが Cisco SoftPhone が動作している装置に接続されていると判断し、VoIP の QoS を自動設定します。  |
| <b>trust</b>           | このポートが信頼できるスイッチまたはルータに接続されていると判断し、自動的に VoIP の QoS を設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッドポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッドポートでは、着信パケットの DSCP 値が信頼されます。 |

## コマンドデフォルト

auto-QoS は、すべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、表 2-2 に示すように、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

表 2-2      トラフィック タイプ、パケット ラベル、およびキュー

|                            | VoIP データ<br>トラフィック  | VoIP Control<br>トラフィック | ルーティング プ<br>ロトコル トラ<br>フィック | STP <sup>1</sup><br>BPDU <sup>2</sup> トラ<br>フィック | リアルタイム<br>ビデオ トラ<br>フィック | その他すべてのトラ<br>フィック                      |
|----------------------------|---------------------|------------------------|-----------------------------|--|--------------------------|--|
| DSCP <sup>3</sup>          | 46                  | 24、26                  | 48                          | 56   | 34                       | —                                      |
| CoS <sup>4</sup>           | 5                   | 3                      | 6                           | 7  | 3                        | —                                      |
| CoS から入力<br>キューへのマッ<br>ピング | 2、3、4、5、6、7 (キュー 2) |                        |                             |  |                          | 0、1 (キュー 1)                            |
| CoS から出力<br>キューへのマッ<br>ピング | 5 (キュー 1)           | 3、6、7 (キュー 2)          |                             |  | 4 (キュー 3)                | 2<br>(キュー<br>3)      0、1<br>(キュー<br>4) |

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

表 2-3 に、入力キューに対して生成された Auto-QoS の設定を示します。

表 2-3 入力キューに対する Auto-QoS の設定

| 入力キュー               | キュー番号 | CoS からキューへのマッピング | キュー ウェイト (帯域幅) | キュー (バッファ) サイズ |
|---------------------|-------|------------------|----------------|----------------|
| SRR <sup>1</sup> 共有 | 1     | 0、1              | 81 %           | 67 %           |
| Priority            | 2     | 2、3、4、5、6、7      | 19 %           | 33 %           |

1. SRR = Shaped Round Robin (シェイプドラウンドロビン)。入力キューは共有モードだけをサポートします。

表 2-4 に、出力キューに対して生成される auto-QoS の設定を示します。

表 2-4 出力キューに対する auto-QoS の設定

| 出力キュー           | キュー番号 | CoS からキューへのマッピング | キュー ウェイト (帯域幅) | ギガビット対応ポートのキュー (バッファ) サイズ | 10/100 イーサネットポートのキュー (バッファ) サイズ |
|-----------------|-------|------------------|----------------|---------------------------|---------------------------------|
| プライオリティ (シェイプド) | 1     | 5                | 最大 100%        | 16 %                      | 10%                             |
| SRR 共有          | 2     | 3、6、7            | 10%            | 6 %                       | 10%                             |
| SRR 共有          | 3     | 2、4              | 60%            | 17 %                      | 26 %                            |
| SRR 共有          | 4     | 0、1              | 20%            | 61 %                      | 54 %                            |

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

LAN Base イメージは、2 つの入力キューと 4 つの出力キューをサポートします。

LAN Lite イメージは、入力キューも出力キューもサポートしません。

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

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

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

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



(注)

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

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

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

- **QoS** がグローバルにイネーブルになり (**mls qos** グローバル コンフィギュレーション コマンド)、そのあと、他のグローバル コンフィギュレーション コマンドが追加されます。  
 スイッチ ポートが Cisco IOS Release 15.0(1) EY で **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを使用して設定された場合、このリリースでは新しい **auto-QoS** によって生成されたコマンドは、ポートに適用されません。このようなコマンドを自動的に適用するには、設定を削除してからポートに再度適用する必要があります。
- **Cisco SoftPhone** が動作する装置に接続されたネットワーク エッジにあるポートに **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチはポリシングを使用してパケットがプロファイル内かプロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という **DSCP** 値がない場合、またはパケットがプロファイル外にある場合、スイッチは **DSCP** 値を 0 に変更します。スイッチは、表 2-3 および表 2-4 の設定に従ってポート上の入力および出力キューを設定します。
- ネットワーク内部に接続されたポート上で、**auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは、入力パケットでルーティングされないポートの **CoS** 値、またはルーテッドポートの **DSCP** 値を信頼します (トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります)。スイッチは、表 2-3 および表 2-4 の設定値に従ってポートの入力キューと出力キューを設定します。

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



(注)

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

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

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

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

### 例

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

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

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

### 関連コマンド

| コマンド  | 説明  |
|---|---|
| <b>debug auto qos</b>   | auto-QoS 機能のデバッグをイネーブルにします。                                   |
| <b>mls qos cos</b>  | デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。 |
| <b>mls qos map {cos-dscp dscp1 ... dscp8   dscp-cos dscp-list to cos}</b> | CoS/DSCP マップまたは DSCP/CoS マップを定義します。                           |
| <b>mls qos queue-set output buffers</b>                                   | バッファをキューセットに割り当てます。   |
| <b>mls qos srr-queue input bandwidth</b>                                  | シェイプド ラウンドロビン (SRR) の重みを入力キューに割り当てます。                         |
| <b>mls qos srr-queue input buffers</b>                                    | 入力キュー間のバッファを割り当てます。   |
| <b>mls qos srr-queue input cos-map</b>                                    | CoS 値を入力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングします。         |
| <b>mls qos srr-queue input dscp-map</b>                                   | DSCP 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングします。       |
| <b>mls qos srr-queue input priority-queue</b>                             | 入力プライオリティ キューを設定し、帯域幅を保証します。                                  |
| <b>mls qos srr-queue output cos-map</b>                                   | CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。          |
| <b>mls qos srr-queue output dscp-map</b>                                  | DSCP 値を出力キュー、またはキューとしきい値 ID にマッピングします。                        |
| <b>mls qos trust queue-set</b>  | ポートの信頼状態を設定します。   |
| <b>queue-set</b>  | ポートをキューセットにマッピングします。  |

| コマンド                                   | 説明  |
|--|---|
| <code>show auto qos</code>             | auto-QoS 情報を表示します。  |
| <code>show mls qos interface</code>    | ポート レベルで QoS 情報を表示します。  |
| <code>srr-queue bandwidth shape</code> | シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。 |
| <code>srr-queue bandwidth share</code> | 共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。         |

# boot buffersize

ファイルシステムでシミュレートした NVRAM のバッファ サイズを指定するには、グローバル コンフィギュレーション モードで **boot buffersize** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**boot buffersize** *size*

**no boot buffersize** *size*

|       |             |   |
|-------|-------------|---|
| 構文の説明 | <i>size</i> | NVRAM のシミュレーション バッファ サイズ。有効な値は 4096 ~ 1048576 です。 |
|-------|-------------|---|

|            |   |
|------------|---|
| コマンド デフォルト | デフォルトのファイル システムでシミュレートした NVRAM のブートのバッファ サイズは 65536 です。 |
|------------|---|

|          |                   |
|----------|-------------------|
| コマンド モード | グローバル コンフィギュレーション |
|----------|-------------------|

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

|   |  |
|---|--|
| 例 | 次に、ファイルシステムでシミュレートした NVRAM のブートのバッファ サイズを 15000 に変更する例を示します。 |
|---|--|

```
Switch(config)# boot buffersize 15000
Switch(config)#
```

| 関連コマンド | コマンド                                 | 説明                                      |
|--------|--------------------------------------|---|
|        | <a href="#">show boot buffersize</a> | ファイルシステムでシミュレートした NVRAM バッファ サイズを表示します。 |

# boot config-file

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込みおよび書き込みに Cisco IOS が使用するファイル名を指定するには、グローバル コンフィギュレーション モードで **boot config-file** コマンドを使用します。デフォルト設定に戻すには、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。

## コマンドデフォルト

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

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 「IE 2000 スイッチのブートローダ 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                  |
|---------------------------|---------------------|
| <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# boot enable-break

自動起動プロセスの中断をイネーブルにするには、グローバル コンフィギュレーション モードで **boot enable-break** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**boot enable-break**

**no boot enable-break**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

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

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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で Break キーを押して、自動ブート プロセスを中断できます。



(注)

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

このコマンドは、ENABLE\_BREAK 環境変数の設定を変更します。詳細については、[付録 A 「IE 2000 スイッチのブートローダ 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                  |
|---------------------------|---------------------|
| <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# boot fast

システム障害発生後のスイッチの起動時間を最適化するには、グローバル コンフィギュレーション モードで **boot fast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**boot fast**

**no boot fast**

## 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

イネーブル

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドはデフォルトでイネーブルになっていますが、システム障害発生後はこの機能は自動的にディセーブルになります。

スイッチの起動時間を最適化し、メモリ テスト、ファイル システム チェック (FSCK)、POST プロセスをディセーブルにするには、このコマンドを使用してブート ファスト機能を再びイネーブルにします。

BOOT 環境変数内の情報を使用して自動的にシステムを起動するようスイッチが設定されている場合、次のリロード シーケンスがすぐに発生します。それ以外は、これらのリロード シーケンスはブート ローダ コンフィギュレーション モードで手動 **boot** コマンドを発行した後に発生します。

### 最初のリロード

このスイッチは **boot fast** 機能をディセーブルにし、次の警告メッセージを表示します。

```
"Reloading with boot fast feature disabled"
```

システム メッセージが表示された後、システムは **crashinfo** を保存し、次のリロードのサイクルのために自動的にリセットされます。

### 2 回目のリロード

ブートローダはフルメモリ テストと LED ステータスの進行状況の FSCK チェックを実行します。メモリ テストと FSCK テストが成功した場合、システムは追加の POST テストを実行し、その結果がコンソールに表示されます。

**boot fast** 機能は、システムが正常に起動した後に再びイネーブルになります。

## 関連コマンド

| コマンド                      | 説明                  |
|---------------------------|---------------------|
| <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# boot helper

ブートローダ初期化中にダイナミックにファイルをロードして、ブートローダの機能を拡張またはパッチを当てるには、グローバル コンフィギュレーション モードで **boot helper** コマンドを使用します。このコマンドをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**boot 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 <b>flash:</b> 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。 |

## コマンド デフォルト

ヘルパー ファイルはロードされません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 「IE 2000 スイッチのブートローダ 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                  |
|---------------------------|---------------------|
| <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# boot 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 ファイルの名前を指定します。これがセット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 によって使用されます。グローバル コンフィギュレーション モードで **boot helper-config-file** コマンドを使用します。デフォルト設定に戻すには、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 <b>flash:</b> 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                          |

## コマンド デフォルト

ヘルパー コンフィギュレーション ファイルは指定されません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 「IE 2000 スイッチのブートローダ 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                  |
|---------------------------|---------------------|
| <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# boot host

ルータ固有のコンフィギュレーション ファイルを最適化するには、グローバル コンフィギュレーション モードで **boot host** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
boot host {dhcp | retry timeout seconds}
```

```
no boot host {dhcp | retry timeout seconds}
```

| 構文の説明 | dhcp            | DHCP を使用してコンフィギュレーション ファイルをダウンロードします。   |
|-------|-----------------|---|
|       | retry           | コンフィギュレーションのダウンロードを再試行します。              |
|       | timeout seconds | タイムアウトを秒単位でセットします。有効な値は 60 ~ 65535 秒です。 |

**コマンドデフォルト** リトライ タイムアウトはディセーブルです。

**コマンドモード** グローバル コンフィギュレーション

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**例** 次に、DHCP を使用してルータ固有のコンフィギュレーション ファイルを最適化する例を示します。

```
Switch(config)# boot host dhcp
Switch(config)#
```

次に、リトライ タイムアウトを 120 秒に再設定する例を示します。

```
Switch(config)# boot host retry timeout 120
Switch(config)#
```

次に、リトライ タイムアウトをディセーブルにする例を示します。

```
Switch(config)# no boot host retry timeout 120
Switch(config)#
```

| 関連コマンド | コマンド                      | 説明                  |
|--------|---------------------------|---------------------|
|        | <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# boot manual

次の起動サイクル時にスイッチの手動による起動をイネーブルにするには、グローバル コンフィギュレーション モードで **boot manual** コマンドを使用します。デフォルト設定に戻すには、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。

## コマンドデフォルト

手動による起動はディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

システムを次回再起動すると、スイッチはブートローダ モードで起動します。これは *switch:* プロンプトによってわかります。システムを起動するには、**boot** ブートローダ 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 「IE 2000 スイッチのブートローダ 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                  |
|---------------------------|---------------------|
| <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# boot private-config-file

プライベート コンフィギュレーションの不揮発性コピーの読み込みおよび書き込みに Cisco IOS が使用するファイル名を指定するには、グローバル コンフィギュレーション モードで **boot private-config-file** コマンドを使用します。デフォルト設定に戻すには、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 |
|-----------------|----------------------------|

## コマンド デフォルト

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

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                  |
|---------------------------|---------------------|
| <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# boot system

Cisco IOS イメージを次の起動サイクル中にロードするように指定するには、グローバル コンフィギュレーション モードで **boot system** コマンドを使用します。デフォルト設定に戻すには、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 <b>flash:</b> 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。                     |

## コマンド デフォルト

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

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 「IE 2000 スイッチのブートローダ 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                  |
|---------------------------|---------------------|
| <a href="#">show boot</a> | BOOT 環境変数の設定を表示します。 |

# channel-group

イーサネット ポートを EtherChannel グループに割り当て、EtherChannel モードをイネーブルにするか、または両方を行うには、インターフェイス コンフィギュレーション モードで **channel-group** 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
```

## 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 ~ 6 です。  |
| <b>mode</b>                 | EtherChannel モードを指定します。  |
| <b>active</b>               | 無条件に Link Aggregation Control Protocol (LACP) をイネーブルにします。<br><br><b>active</b> 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、 <b>active</b> モードまたは <b>passive</b> モードの別のポート グループで形成されます。                            |
| <b>auto</b>                 | ポート集約プロトコル (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。<br><br><b>auto</b> 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、 <b>desirable</b> モードの別のポート グループでだけ形成されます。 <b>auto</b> 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。 |
| <b>desirable</b>            | PAgP を無条件にイネーブルにします。<br><br><b>desirable</b> モードは、ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。EtherChannel は、 <b>desirable</b> モードまたは <b>auto</b> モードの別のポート グループで形成されます。 <b>desirable</b> 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。    |
| <b>non-silent</b>           | (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 <b>auto</b> または <b>desirable</b> キーワードとともに使用されます。  |

|                |   |
|----------------|---|
| <b>on</b>      | on モードをイネーブルにします。<br><br>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。  |
| <b>passive</b> | 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。<br><br>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。 |

**コマンドデフォルト**

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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**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。

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、物理ポート上で稼働している 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**

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

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 が稼働している複数の 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。

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

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

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

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

**注意**

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

**例**

次に、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 gigabitethernet1/1 -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 gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

## ■ channel-group

## 関連コマンド

| コマンド                                   | 説明                                   |
|--|--------------------------------------|
| <a href="#">channel-protocol</a>       | 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。 |
| <a href="#">interface port-channel</a> | 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。    |
| <a href="#">show etherchannel</a>      | チャネルの EtherChannel 情報を表示します。         |
| <a href="#">show lacp</a>              | LACP チャネル グループ情報を表示します。              |
| <a href="#">show pagp</a>              | PAgP チャネル グループ情報を表示します。              |

# 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するには、インターフェイス コンフィギュレーション モードで **channel-protocol** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**channel-protocol {lACP | pAgP}**

**no channel-protocol**

## 構文の説明

|             |   |
|-------------|---|
| <b>lACP</b> | Link Aggregation Control Protocol (LACP) で EtherChannel を設定します。 |
| <b>pAgP</b> | ポート集約プロトコル (PAgP) で EtherChannel を設定します。                        |

## コマンド デフォルト

EtherChannel に割り当てられているプロトコルはありません。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

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

EtherChannel グループ上で、PAgP および LACP モードの両方をイネーブルにすることはできません。PAgP と LACP には互換性がありません。両方ともチャネルの終端は同じプロトコルを使用する必要があります。

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

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

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

## 関連コマンド

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

# cip enable

VLAN の Common Industrial Protocol (CIP) をイネーブルにするには、インターフェイス コンフィギュレーション モードで **cip enable** コマンドを使用します。CIP 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。

**cip enable**

**no cip enable**

## 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

デフォルトでは、すべての VLAN で CIP はディセーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

インターフェイスには物理インターフェイスではなく、VLAN を使用します。

CIP はスイッチの VLAN で 1 つのみイネーブルにできます。

CIP をイネーブルにする際は、CIP セキュリティ パスワードを設定することを推奨します。

## 例

次に、VLAN 3 で CIP をイネーブルにする例を示します。

```
Switch(config)# interface vlan 20
Switch(config-if)# cip enable
```

次の例では、2 つめの VLAN で CIP をイネーブルにしようとする则表示されるメッセージを示します。

```
Switch(config)# interface vlan 3
Switch(config-if)# cip enable
CIP is already enabled on Vlan 20
```

## 関連コマンド

| コマンド                         | 説明                      |
|------------------------------|-------------------------|
| <a href="#">cip security</a> | CIP セキュリティ オプションを設定します。 |
| <a href="#">show cip</a>     | CIP サブシステムに関する情報を表示します。 |

# cip security

スイッチに Common Industrial Protocol (CIP) セキュリティ オプションを設定するには、グローバル コンフィギュレーション モードで **cip security** コマンドを使用します。パスワードの中止またはタイムアウト値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。

**cip security** {**password** *password* | **window timeout** *value*}

**no cip security** {**password** *password* | **window timeout**}

## 構文の説明

|                                 |  |
|---------------------------------|--|
| <b>password</b> <i>password</i> | CIP セキュリティの ASCII パスワードを設定します。                                       |
| <b>window timeout</b>           | CIP セキュリティ ウィンドウのタイムアウトを設定します。                                       |
| <i>value</i>                    | CIP セキュリティ ウィンドウのタイムアウト値を設定します。指定できる範囲は 1 ~ 3600 秒です。デフォルトは 600 秒です。 |

## コマンド デフォルト

パスワードは設定されていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

VLAN で CIP をイネーブルにする際は、CIP セキュリティ パスワードを設定することを推奨します。設定しないと、すべての CIP ユーザがスイッチを設定できます。

## 例

次の例では、CIP セキュリティ ウィンドウのタイムアウト値を 1 時間に設定する方法を示します。

```
Switch(config)# cip security window timeout 3600
```

次の例では、CIP セキュリティ パスワードを 123 に設定する方法を示します。

```
Switch(config)# cip security password abc123
```

## 関連コマンド

| コマンド              | 説明                      |
|-------------------|-------------------------|
| <b>cip enable</b> | VLAN 上で CIP をイネーブルにします。 |
| <b>show cip</b>   | CIP サブシステムに関する情報を表示します。 |

# cisp enable

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スイッチの Client Information Signalling Protocol (CISP) をイネーブルにするには、グローバル コンフィギュレーション モードで **cisp enable** コマンドを使用します。

**cisp enable**

**no cisp enable**

## 構文の説明

**cisp enable** CISP をイネーブルにします。

## コマンドデフォルト

なし

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

オーセンティケータとサブリカントスイッチの間のリンクはトランクです。両方のスイッチで VTP をイネーブルにする場合は、VTP ドメイン名が同一であり、VTP モードがサーバである必要があります。

VTP モードを設定する場合は、MD5 チェックサムの一貫性エラーにならないようにするために、次の点を確認してください。

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

## 例

次の例では、CISP をイネーブルにする方法を示します。

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

## 関連コマンド

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

# class

指定のクラスマップ名のトラフィック分類の一致基準を (**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドを使用して) 定義するには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。既存のクラス マップを削除する場合は、このコマンドの **no** 形式を使用します。

```
class class-map-name
```

```
no class class-map-name
```

## 構文の説明

*class-map-name* クラス マップ名です。

## コマンドデフォルト

ポリシー マップ クラス マップは定義されていません。

## コマンドモード

ポリシー マップ コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

**class** コマンドを入力すると、ポリシー マップ クラス コンフィギュレーション モードに入り、次のコンフィギュレーション コマンドが使用可能になります。

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

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

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

## 例

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

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

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   |
|------------------------------|--|
| <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>police</code>          | 分類したトラフィックにポリサーを定義します。   |
| <code>policy-map</code>      | 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。   |
| <code>set</code>             | パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。  |
| <code>show policy-map</code> | Quality of Service (QoS) ポリシー マップを表示します。   |
| <code>trust</code>           | <code>class</code> ポリシーマップ コンフィギュレーション コマンドまたは <code>class-map</code> グローバル コンフィギュレーション コマンドを使用して分類されたトラフィックの信頼状態を定義します。 |

# class-map

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

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

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

## 構文の説明

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

## コマンド デフォルト

クラス マップは定義されていません。

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

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

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

Quality of Service (QoS) クラスマップ コンフィギュレーション モードでは、次のコンフィギュレーション コマンドを利用することができます。

- **description** : クラス マップを説明します (最大 200 文字)。**show class-map** 特権 EXEC コマンドは、クラスマップの説明と名前を表示します。
- **exit** : QoS クラスマップ コンフィギュレーション モードを終了します。
- **match** : 分類基準を設定します。詳細については、**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。
- **rename** : 現在のクラス マップの名前を変更します。クラス マップ名をすでに使用されている名前に変更すると、「A class-map with this name already exists」というメッセージが表示されません。

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

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

**例**

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

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

次の例では、クラス マップ `class1` を削除する方法を示します。

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

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

**関連コマンド**

| コマンド                              | 説明   |
|-----------------------------------|--|
| <b>class</b>                      | 指定されたクラスマップ名のトラフィック分類一致条件 ( <b>police</b> 、 <b>set</b> 、および <b>trust</b> ポリシー マップ クラス コンフィギュレーション コマンドによる) を定義します。 |
| <b>match</b> (クラスマップ コンフィギュレーション) | トラフィックを分類するための一致条件を定義します。  |
| <b>policy-map</b>                 | 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。  |
| <b>show class-map</b>             | QoS クラス マップを表示します。   |

# clear dot1x

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

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

| 構文の説明 | all                              | interface interface-id               |
|-------|----------------------------------|--------------------------------------|
|       | スイッチのすべての IEEE 802.1x 情報をクリアします。 | 指定したインターフェイスの IEEE 802.1x 情報をクリアします。 |

コマンド 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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

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

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

```
Switch# clear dot1x all
```

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

```
Switch# clear dot1x interface gigabithernet1/1
```

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

| 関連コマンド | コマンド                       | 説明  |
|--------|----------------------------|---|
|        | <a href="#">show dot1x</a> | スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。 |

# clear eap sessions

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

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

## 構文の説明

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

## コマンドデフォルト

なし

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

## 例

次の例では、すべての EAP 情報をクリアする方法を示します。

```
Switch# clear eap
```

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

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

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

## 関連コマンド

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

# clear errdisable interface

errdisable になっている VLAN を再びイネーブルにするには、特権 EXEC モードで **clear errdisable interface** コマンドを使用します。

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

## 構文の説明

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

## コマンド デフォルト

なし

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

## 例

次に、ポート 2 で errdisable になっているすべての VLAN を再びイネーブルにする例を示します。

```
Switch# clear errdisable interface GigabitEthernet1/2 vlan
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">errdisable detect cause</a>             | 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。            |
| <a href="#">errdisable recovery</a>                 | 回復メカニズム変数を設定します。  |
| <a href="#">show errdisable detect</a>              | errdisable 検出ステータスを表示します。                               |
| <a href="#">show errdisable recovery</a>            | errdisable 回復タイマーの情報を表示します。                             |
| <a href="#">show interfaces status err-disabled</a> | errdisable ステートになっているインターフェイスのリストのインターフェイス ステータスを表示します。 |

# clear arp inspection log

ダイナミックな Address Resolution Protocol (ARP) インスペクション ログ バッファをクリアするには、特権 EXEC モードで **clear ip arp inspection log** 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。

### コマンドデフォルト

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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                                       |
|--|--|
| <a href="#">arp access-list</a>                | ARP アクセス コントロール リスト (ACL) を定義します。        |
| <a href="#">ip arp inspection log-buffer</a>   | ダイナミック ARP インスペクション ログ バッファを設定します。       |
| <a href="#">ip arp inspection vlan logging</a> | VLAN 単位で記録するパケットのタイプを制御します。              |
| <a href="#">show inventory log</a>             | ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。 |

# clear ip arp inspection statistics

ダイナミックな Address Resolution Protocol (ARP) インスペクション統計情報をクリアするには、特権 EXEC モードで **clear ip arp inspection statistics** コマンドを使用します。

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

|           |  |  |
|-----------|--|--|
| 構文の説明     | <b>vlan vlan-range</b>   | (任意) 指定した 1 つ以上の VLAN の統計情報をクリアします。<br><br>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。 |
| コマンドデフォルト | なし   |  |
| コマンドモード   | 特権 EXEC  |  |
| コマンド履歴    | <b>リリース</b>  | <b>変更内容</b>  |
|           | 15.0(1)EY  | このコマンドが導入されました。  |
| 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。<br>Switch# <b>clear ip arp inspection statistics vlan 1</b><br><br>統計情報が削除されたかどうかを確認するには、 <b>show ip arp inspection statistics vlan 1</b> 特権 EXEC コマンドを入力します。 |  |
| 関連コマンド    | <b>コマンド</b>  | <b>説明</b>  |
|           | <a href="#">show inventory statistics</a>  | すべての VLAN または指定された VLAN の転送済みパケット、ドロップ済みパケット、MAC 検証に失敗したパケット、および IP 検証に失敗したパケットの統計情報を表示します。  |

# clear ip dhcp snooping

DHCP スヌーピング バインディング データベース、DHCP スヌーピング バインディング データベース エージェント統計情報、または DHCP スヌーピング統計カウンタをクリアするには、特権 EXEC モードで **clear ip dhcp snooping** 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

|                               |  |
|-------------------------------|--|
| <b>binding</b>                | DHCP スヌーピング バインディング データベースを消去します。              |
| *                             | すべての自動バインディングをクリアします。                          |
| <b>ip-address</b>             | バインディング エントリ IP アドレスをクリアします。                   |
| <b>interface interface-id</b> | バインディング入力インターフェイスをクリアします。                      |
| <b>vlan vlan-id</b>           | バインディング エントリ VLAN をクリアします。                     |
| <b>database statistics</b>    | 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。 |
| <b>statistics</b>             | DHCP スヌーピング統計カウンタをクリアします。                      |

## コマンドデフォルト

なし

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 関連コマンド

| コマンド   | 説明  |
|--|---|
| <a href="#">ip dhcp snooping</a>                 | VLAN 上で DHCP スヌーピングをイネーブルにします。                          |
| <a href="#">ip dhcp snooping database</a>        | 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。 |
| <a href="#">show ip dhcp snooping binding</a>    | 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。                  |
| <a href="#">show ip dhcp snooping database</a>   | 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。           |
| <a href="#">show ip dhcp snooping statistics</a> | DHCP スヌーピングの統計情報を表示します。                                 |

# clear ipc

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

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



(注)

このコマンドは、スイッチで IP サービス イメージが稼働されている場合にのみ表示されます。

## 構文の説明

|                         |                     |
|-------------------------|---------------------|
| <b>queue-statistics</b> | すべてのキュー統計情報をクリアします。 |
| <b>statistics</b>       | 統計情報をクリアします。        |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                             |
|---------------------------------|--------------------------------|
| <b>show ipc {rpc   session}</b> | 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、特権 EXEC モードで **clear ipv6 dhcp conflict** コマンドを使用します。

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



(注)

このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

## 構文の説明

|              |                                  |
|--------------|----------------------------------|
| *            | すべてのアドレス競合。                      |
| 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。 |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

競合を検出するように DHCPv6 サーバを設定する場合、DHCPv6 サーバは ping を使用します。クライアントは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ることができません。

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

## 例

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

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

## 関連コマンド

| コマンド                                    | 説明   |
|---|--|
| <a href="#">show ipv6 dhcp conflict</a> | 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 lacp

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

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

## 構文の説明

|                             |                                  |
|-----------------------------|----------------------------------|
| <i>channel-group-number</i> | チャンネル グループ番号。指定できる範囲は 1 ~ 48 です。 |
| <b>counters</b>             | トラフィック カウンタをクリアします。              |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                       |
|---------------------------|--------------------------|
| <a href="#">show lacp</a> | LACP チャンネル グループ情報を表示します。 |

# clear mac address-table

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 アドレスを削除するには、特権 EXEC モードで **clear mac address-table** 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

|                               |   |
|-------------------------------|---|
| <b>dynamic</b>                | すべてのダイナミック MAC アドレスを削除します。                                      |
| <b>address mac-addr</b>       | (任意) 指定したダイナミック MAC アドレスを削除します。                                 |
| <b>interface interface-id</b> | (任意) 指定し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。           |
| <b>vlan vlan-id</b>           | (任意) 指定した VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ~ 4094 です。 |
| <b>notification</b>           | 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。                                    |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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  |
|---|---|
| <a href="#">mac address-table notification</a>      | MAC アドレス通知機能をイネーブルにします。                                       |
| <a href="#">show mac access-group</a>               | 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。                |
| <a href="#">show mac address-table notification</a> | 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。          |
| <a href="#">snmp trap mac-notification change</a>   | 特定のインターフェイス上の簡易ネットワーク管理プロトコル (SNMP) 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 テーブル移行更新関連カウンタをクリアするには、特権 EXEC モードで **clear mac address-table move update** コマンドを使用します。

## clear mac address-table move update

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドデフォルト

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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                               |
|--|----------------------------------|
| <a href="#">mac address-table move update {receive   transmit}</a> | 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。  |
| <a href="#">show mac address-table move update</a>                 | スイッチに MAC アドレス テーブル移行更新情報を表示します。 |

# clear nmsp statistics

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

## clear nmsp statistics

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 例

次の例では、NMSP の統計情報をクリアする方法を示します。

```
Switch# clear nmsp statistics
```

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

### 関連コマンド

| コマンド                      | 説明             |
|---------------------------|----------------|
| <a href="#">show nmsp</a> | NMSP 情報を表示します。 |

# clear pagp

ポート集約プロトコル (PAgP) のチャンネル グループ情報をクリアするには、特権 EXEC モードで **clear pagp** コマンドを使用します。

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

## 構文の説明

|                             |                                 |
|-----------------------------|---------------------------------|
| <i>channel-group-number</i> | チャンネル グループ番号。指定できる範囲は 1 ~ 6 です。 |
| <b>counters</b>             | トラフィック カウンタをクリアします。             |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                       |
|---------------------------|--------------------------|
| <a href="#">show pagp</a> | PAgP チャンネル グループ情報を表示します。 |

# clear port-security

MAC アドレス テーブルからすべてのセキュア アドレスを削除するか、スイッチまたはインターフェイス上の特定のタイプ (configured、dynamic、または sticky) のすべてのセキュア アドレスを削除するには、特権 EXEC モードで **clear port-security** 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

|                               |  |
|-------------------------------|--|
| <b>all</b>                    | すべてのセキュア MAC アドレスを削除します。   |
| <b>configured</b>             | 設定済みセキュア MAC アドレスを削除します。   |
| <b>dynamic</b>                | 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。  |
| <b>sticky</b>                 | 自動学習または設定済みのいずれかのセキュア MAC アドレスを削除します。  |
| <b>address mac-addr</b>       | (任意) 指定したダイナミック セキュア MAC アドレスを削除します。   |
| <b>interface interface-id</b> | (任意) 指定し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。   |
| <b>vlan</b>                   | (任意) 指定した VLAN から指定したセキュア MAC アドレスを削除します。 <b>vlan</b> 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"> <li><b>vlan-id</b> : 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。</li> <li><b>access</b> : アクセス ポートで、アクセス VLAN 上の指定したセキュア MAC アドレスをクリアします。</li> <li><b>voice</b> : アクセス ポートで、音声 VLAN 上の指定したセキュア MAC アドレスをクリアします。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合に限り利用可能です。</p> |

コマンド デフォルト なし

コマンド モード 特権 EXEC

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

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
```

## clear port-security

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

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

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                                       |
|---|--|
| <b>switchport port-security</b>                         | 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。          |
| <b>switchport port-security mac-address mac-address</b> | セキュア MAC アドレスを設定します。                     |
| <b>switchport port-security maximum value</b>           | 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。   |
| <b>show port-security</b>                               | 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 psp counter

すべてのプロトコルについてドロップされたパケットのプロトコル ストーム プロテクション カウンタをクリアするには、特権 EXEC モードで **clear psp counter** コマンドを使用します。

**clear psp counter [arp | igmp | dhcp]**

| 構文の説明       |  |
|-------------|--|
| <b>arp</b>  | (任意) ARP および ARP スヌーピングのドロップされたパケットのカウンタをクリアします。   |
| <b>dhcp</b> | (任意) DHCP および DHCP スヌーピングのドロップされたパケットのカウンタをクリアします。 |
| <b>igmp</b> | (任意) IGMP および IGMP スヌーピングのドロップされたパケットのカウンタをクリアします。 |

**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       | 変更内容            |
|--------|------------|-----------------|
|        | 15.0(58)SE | このコマンドが導入されました。 |

**例** この例では、DHCP のプロトコル ストーム プロテクション カウンタがクリアされます。

```
Switch# clear psp counter dhcp
Switch#
```

| 関連コマンド | コマンド                       | 説明   |
|--------|----------------------------|--|
|        | <b>psp</b>                 | ARP、DHCP、または IGMP のプロトコル ストーム プロテクションを設定します。 |
|        | <b>show psp config</b>     | プロトコル ストーム プロテクションの設定を表示します。                 |
|        | <b>show psp statistics</b> | ドロップされたパケットの数を表示します。                         |

# 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) カウンタをクリアするには、特権 EXEC モードで **clear rep counters** 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。

## コマンドデフォルト

なし

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                          |
|--|-----------------------------|
| <a href="#">show interfaces rep detail</a> | REP の設定およびステータス情報の詳細を表示します。 |

# clear spanning-tree counters

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

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

| 構文の説明                              | <b>interface interface-id</b> (任意) 指定のインターフェイスのスパニングツリー カウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN、ポートチャネルなどがあります。指定できる VLAN 範囲は 1 ~ 4094 です。ポートチャネルの範囲は 1 ~ 6 です。 |      |      |                                    |                        |
|------------------------------------|---|------|------|------------------------------------|------------------------|
| コマンド デフォルト                         | なし  |      |      |                                    |                        |
| コマンド モード                           | 特権 EXEC   |      |      |                                    |                        |
| コマンド履歴                             | <table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>15.0(1)EY</td><td>このコマンドが導入されました。</td></tr></tbody></table>                               | リリース | 変更内容 | 15.0(1)EY                          | このコマンドが導入されました。        |
| リリース                               | 変更内容  |      |      |                                    |                        |
| 15.0(1)EY                          | このコマンドが導入されました。   |      |      |                                    |                        |
| 使用上のガイドライン                         | <i>interface-id</i> 値が指定されていない場合は、すべてのインターフェイスのスパニングツリー カウンタがクリアされます。   |      |      |                                    |                        |
| 例                                  | 次の例では、すべてのインターフェイスのスパニングツリー カウンタをクリアする方法を示します。<br>Switch# <b>clear spanning-tree counters</b>   |      |      |                                    |                        |
| 関連コマンド                             | <table><thead><tr><th>コマンド</th><th>説明</th></tr></thead><tbody><tr><td><a href="#">show spanning-tree</a></td><td>スパニングツリー ステート情報を表示します。</td></tr></tbody></table> | コマンド | 説明   | <a href="#">show spanning-tree</a> | スパニングツリー ステート情報を表示します。 |
| コマンド                               | 説明  |      |      |                                    |                        |
| <a href="#">show spanning-tree</a> | スパニングツリー ステート情報を表示します。  |      |      |                                    |                        |

# clear spanning-tree detected-protocols

すべてのインターフェイスまたは指定したインターフェイスでプロトコル移行プロセスを再開（強制的に近接スイッチと再びネゴシエートさせる）するには、特権 EXEC モードで **clear spanning-tree detected-protocols** 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) 指定したインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスとしては、物理ポート、VLAN、ポートチャネルなどがあります。指定できる VLAN 範囲は 1 ~ 4094 です。ポートチャネル範囲は 1 ~ 6 です。

## コマンドデフォルト

なし

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

Rapid Per-VLAN Spanning-Tree Plus (RPVST+) プロトコルまたは Multiple Spanning Tree Protocol (MSTP) が稼働するスイッチは、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。RPVST+ 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ブリッジプロトコルデータユニット (BPDU) 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。マルチスパンニングツリー (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)、または高速スパンニングツリー (RST) 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も検出できます。

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

## 例

次に、ギガビットイーサネットポート上でプロトコル移行プロセスを再開する例を示します。

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet1/1
```

次に、ファストイーサネットポートでプロトコル移行プロセスを再開する例を示します。

```
Switch# clear spanning-tree detected-protocols interface fastethernet1/1
```

## 関連コマンド

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

# clear vmps statistics

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

## clear vmps statistics

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドデフォルト

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 例

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

```
Switch# clear vmps statistics
```

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

### 関連コマンド

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

# clear vtp counters

VLAN トランキンク プロトコル (VTP) とプルーニング カウンタをクリアするには、特権 EXEC モードで **clear vtp counters** コマンドを使用します。

**clear vtp counters**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、VTP カウンタをクリアする方法を示します。

```
Switch# clear vtp counters
```

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

## 関連コマンド

| コマンド                     | 説明                                |
|--------------------------|-----------------------------------|
| <a href="#">show vtp</a> | VTP 管理ドメイン、ステータス、カウンタの一般情報を表示します。 |

# cluster commander-address

クラスタ メンバ スイッチがクラスタに加入した場合に、MAC アドレスをそのクラスタ メンバ スイッチに自動的に提供するには、グローバル コンフィギュレーション モードの **cluster commander-address** コマンドを使用します。デバッグまたはリカバリ手順の間だけスイッチをクラスタから削除する場合は、クラスタ メンバ スイッチ コンソール ポートから、このコマンドの **no** 形式を使用します。

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

**no cluster commander-address**

## 構文の説明

|                      |  |
|----------------------|--|
| <i>mac-address</i>   | クラスタ コマンド スイッチの MAC アドレス                             |
| <b>member number</b> | (任意) 設定されたクラスタ メンバ スイッチの番号を指定します。指定できる範囲は 0 ~ 15 です。 |
| <b>name name</b>     | (任意) 設定されたクラスタの名前を指定します (最大 31 文字)。                  |

## コマンド デフォルト

このスイッチはどのクラスタのメンバでもありません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、スタンドアロンクラスタ メンバ スイッチから入力する必要はありません。クラスタ コマンド スイッチは、メンバ スイッチがクラスタに加入した場合に、MAC アドレスをそのメンバ スイッチに自動的に提供します。クラスタ メンバ スイッチは、この情報および他のクラスタ情報をその実行コンフィギュレーション ファイルに追加します。

このコマンドは、クラスタ コマンド スイッチ上でだけ使用できます。

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

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

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

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

**例**

次の例では、実行中のクラスタ メンバの設定から、その出力を一部示します。

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

<output truncated>

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

<output truncated>

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

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

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

**関連コマンド**

| コマンド                          | 説明                               |
|-------------------------------|----------------------------------|
| <a href="#">debug cluster</a> | スイッチが属するクラスタのステータスおよびサマリーを表示します。 |

# cluster discovery hop-count

候補スイッチの拡張検出を行うためのホップカウント制限を設定するには、クラスタ コマンド スイッチ上のグローバル コンフィギュレーション モードで **cluster discovery hop-count** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**cluster discovery hop-count** *number*

**no cluster discovery hop-count**

## 構文の説明

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

## コマンドデフォルト

ホップ カウントは 3 に設定されています。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

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

## 例

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

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

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

## 関連コマンド

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

# cluster enable

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

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

**no cluster enable**

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

**コマンド デフォルト** このスイッチはクラスタ コマンド スイッチではありません。  
 クラスタ名は定義されません。  
 スイッチがクラスタ コマンド スイッチである場合、メンバ番号は 0 です。

**コマンド モード** グローバル コンフィギュレーション

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン** このコマンドは、どのクラスタにも属していない任意のコマンド対応スイッチ上で入力します。装置がすでにクラスタのメンバとして設定されている場合、コマンドはエラーとなります。  
 クラスタ コマンド スイッチをイネーブルにするときには、クラスタに名前を付けてください。スイッチがすでにクラスタ コマンド スイッチとして設定されており、クラスタ名が以前の名前と異なっている場合、コマンドはクラスタ名を変更します。

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

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

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

| 関連コマンド | コマンド                         | 説明                               |
|--------|------------------------------|----------------------------------|
|        | <a href="#">show cluster</a> | スイッチが属するクラスタのステータスおよびサマリーを表示します。 |

# cluster holdtime

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

**cluster holdtime holdtime-in-secs**

**no cluster holdtime**

## 構文の説明

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

## コマンドデフォルト

デフォルトのホールド時間は 80 秒です。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

クラスタ コマンド スイッチ上でだけ、このコマンドと **cluster timer** グローバル コンフィギュレーション コマンドを入力してください。クラスタ内のすべてのスイッチ間で設定の一貫性が保たれるように、クラスタ コマンド スイッチはこの値をそのすべてのクラスタ メンバに伝達します。

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

## 例

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

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

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

## 関連コマンド

| コマンド                         | 説明                               |
|------------------------------|----------------------------------|
| <a href="#">show cluster</a> | スイッチが属するクラスタのステータスおよびサマリーを表示します。 |

# cluster member

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

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

**no cluster member** *n*

## 構文の説明

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

## コマンド デフォルト

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

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

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

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

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

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

## 例

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

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

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

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

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

## 関連コマンド

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

# cluster outside-interface

クラスタのネットワーク アドレス変換 (NAT) の外部インターフェイスを設定し、IP アドレスのないメンバがクラスタの外部にある装置と通信できるようにするには、グローバル コンフィギュレーション モードで **cluster outside-interface** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**cluster outside-interface** *interface-id*

**no cluster outside-interface**

## 構文の説明

*interface-id* 外部インターフェイスとして機能するインターフェイス。有効なインターフェイスとしては、物理インターフェイス、ポート チャネル、または VLAN があります。ポート チャネル範囲は 1 ~ 6 です。指定できる VLAN 範囲は 1 ~ 4094 です。

## コマンド デフォルト

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

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

## 例

次の例では、VLAN 1 に外部インターフェイスを設定する方法を示します。

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

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

## 関連コマンド

| コマンド                       | 説明   |
|----------------------------|--|
| <b>show running-config</b> | 現在の動作設定を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# cluster run

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

**cluster run**

**no cluster run**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

すべてのスイッチでクラスタリングがイネーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

クラスタ コマンド スイッチ上で **no cluster run** コマンドを入力すると、クラスタ コマンド スイッチはディセーブルになります。クラスタリングはディセーブルになり、スイッチは候補スイッチになることができません。

クラスタ メンバ スイッチで **no cluster run** コマンドを入力すると、このメンバ スイッチはクラスタから削除されます。クラスタリングはディセーブルになり、スイッチは候補スイッチになることができません。

クラスタに属していないスイッチで **no cluster run** コマンドを入力すると、クラスタリングはそのスイッチ上でディセーブルになります。このスイッチは候補スイッチになることができません。

## 例

次の例では、クラスタ コマンド スイッチでクラスタリングをディセーブルにする方法を示します。

```
Switch(config)# no cluster run
```

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

## 関連コマンド

| コマンド                         | 説明                               |
|------------------------------|----------------------------------|
| <a href="#">show cluster</a> | スイッチが属するクラスタのステータスおよびサマリーを表示します。 |

# cluster standby-group

既存の Hot Standby Router Protocol (HSRP) にクラスタをバインドして、クラスタ コマンド スイッチの冗長性をイネーブルにするには、グローバル コンフィギュレーション モードで **cluster standby-group** コマンドを使用します。routing-redundancy キーワードを入力することで、同一の HSRP グループが、クラスタ コマンド スイッチの冗長性およびルーティングの冗長性に対して使用できるようになります。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**cluster standby-group** *HSRP-group-name* [**routing-redundancy**]

**no cluster standby-group**

## 構文の説明

|                           |  |
|---------------------------|--|
| <i>HSRP-group-name</i>    | クラスタにバインドされる HSRP グループの名前。設定できるグループ名は 32 文字までです。                           |
| <b>routing-redundancy</b> | (任意) 同一の HSRP スタンバイ グループをイネーブルにし、クラスタ コマンド スイッチの冗長性およびルーティングの冗長性に対して使用します。 |

## コマンド デフォルト

クラスタは、どの HSRP グループにもバインドされません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

クラスタ コマンド スイッチは、クラスタ HSRP バインディング情報をすべてのクラスタ HSRP 対応メンバに伝播します。各クラスタ メンバ スイッチはバインディング情報を NVRAM に保存します。HSRP グループ名は、有効なスタンバイ グループである必要があります。そうでない場合、エラーが発生してコマンドが終了します。

クラスタにバインドする HSRP スタンバイ グループのすべてのメンバに同じグループ名を使用する必要があります。バインドされる HSRP グループのすべてのクラスタ HSRP 対応メンバに同じ HSRP グループ名を使用してください (クラスタを HSRP グループにバインドしない場合には、クラスタ コマンドおよびメンバに異なる名前を使用できます)。

## 例

次の例では、**my\_hsrp** という名前の HSRP グループをクラスタにバインドする方法を示します。このコマンドは、クラスタ コマンド スイッチ上から実行します。

```
Switch(config)# cluster standby-group my_hsrp
```

次の例では、同じ HSRP グループ名 **my\_hsrp** を使用して、ルーティング冗長とクラスタ冗長を確立する方法を示します。

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
```

## cluster standby-group

次の例では、このコマンドがクラスタ コマンド スイッチから実行され、指定された HSRP スタンバイグループが存在しない場合のエラー メッセージを示します。

```
Switch(config)# cluster standby-group my_hsrp
%ERROR: Standby (my_hsrp) group does not exist
```

次の例では、このコマンドがクラスタ メンバ スイッチで実行された場合のエラー メッセージを示します。

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
%ERROR: This command runs on a cluster command switch
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。出力は、クラスタ内の冗長性がイネーブルになったかどうかを示します。

## 関連コマンド

| コマンド                | 説明  |
|---------------------|---|
| <b>standby ip</b>   | インターフェイスで HSRP をイネーブルにします。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show cluster</b> | スイッチが属するクラスタのステータスおよびサマリーを表示します。  |
| <b>show standby</b> | スタンバイ グループ情報を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。        |

# cluster timer

ハートビートメッセージの間隔を秒単位で設定するには、グローバル コンフィギュレーション モードで **cluster timer** コマンドを使用します。デフォルト値の間隔を設定する場合は、このコマンドの **no** 形式を使用します。

**cluster timer** *interval-in-secs*

**no cluster timer**

|              |                         |   |
|--------------|-------------------------|---|
| <b>構文の説明</b> | <i>interval-in-secs</i> | ハートビートメッセージ間隔 (秒)。指定できる範囲は 1 ~ 300 秒です。 |
|--------------|-------------------------|---|

|                  |          |
|------------------|----------|
| <b>コマンドデフォルト</b> | 8 秒間隔です。 |
|------------------|----------|

|                |                   |
|----------------|-------------------|
| <b>コマンドモード</b> | グローバル コンフィギュレーション |
|----------------|-------------------|

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

|                   |  |
|-------------------|--|
| <b>使用上のガイドライン</b> | このコマンドと <b>cluster holdtime</b> グローバル コンフィギュレーション コマンドは、クラスタ コマンド スイッチ上に限り入力してください。クラスタ内のすべてのスイッチ間で設定の一貫性が保たれるように、クラスタ コマンド スイッチはこの値をそのすべてのクラスタ メンバに伝達します。 |
|-------------------|--|

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

|          |  |
|----------|--|
| <b>例</b> | 次の例では、クラスタ コマンド スイッチでハートビート間隔のタイマーおよび期間を変更する方法を示します。 |
|----------|--|

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

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

| 関連コマンド | コマンド                         | 説明                               |
|--------|------------------------------|----------------------------------|
|        | <a href="#">show cluster</a> | スイッチが属するクラスタのステータスおよびサマリーを表示します。 |

# define interface-range

インターフェイスレンジマクロを作成するには、グローバル コンフィギュレーション モードで **define interface-range** 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値については、「Usage Guidelines（使用上のガイドライン）」を参照してください。 |

## コマンド デフォルト

なし

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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て行うことができます。

*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、**gigabitethernet1/1 - 2** は有効な範囲ですが、**gigabitethernet 1/1-2** は無効な範囲です。

*type* および *interface* の有効値は次のとおりです。

- **vlan vlan-id - vlan-ID**（VLAN ID は 1 ～ 4094）

VLAN インターフェイスは、**interface vlan** コマンドで設定する必要があります（**show running-config** 特権 EXEC コマンドは、設定された VLAN インターフェイスを表示します）。**show running-config** コマンドで表示されない VLAN インターフェイスは、*interface-range* では使用できません。

- **port-channel port-channel-number**。ここで、*port-channel-number* は 1 ～ 6 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。
- 範囲は、*type number/number - number* です（例：**gigabitethernet1/1 - 2**）。

範囲を定義するときは、ハイフン (-) の前にスペースが必要です。次に例を示します。

**gigabitethernet1/1 - 2**

複数の範囲を入力することもできます。複数の範囲を定義するときは、カンマ (,) の前の最初のエントリの後にスペースを入力する必要があります。カンマの後のスペースは任意になります。次に例を示します。

**fastethernet1/3, gigabitethernet1/1 - 2**

**fastethernet1/3 -4, gigabitethernet1/1 - 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 macrol fastethernet1/1 - 2, gigabitethernet1/1 - 2
```

## 関連コマンド

| コマンド                                | 説明   |
|-------------------------------------|--|
| <a href="#">interface range</a>     | 複数のポートで 1 つのコマンドを同時に実行します。   |
| <a href="#">show running-config</a> | 定義されたマクロを含む現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# delete

フラッシュ メモリ デバイス上のファイルまたはディレクトリを削除するには、特権 EXEC モードで **delete** コマンドを使用します。

```
delete [/force] [/recursive] filesystem:/file-url
```

## 構文の説明

|                    |  |
|--------------------|--|
| <b>/force</b>      | (任意) 削除を確認するプロンプトを抑制します。   |
| <b>/recursive</b>  | (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。           |
| <b>filesystem:</b> | フラッシュ ファイル システムのエイリアスです。<br>ローカル フラッシュ ファイル システムの構文<br><b>flash:</b> |
| <b>/file-url</b>   | 削除するパス (ディレクトリ) およびファイル名   |

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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  |
|-------------------------------------|---|
| <a href="#">archive download-sw</a> | 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一致に基づいて ARP パケットを拒否するには、アドレス解決プロトコル (ARP) のアクセスリスト 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。アクセスリストから指定されたアクセス コントロール エントリ (ACE) を削除するには、このコマンドの **no** 形式を使用します。

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

```
no deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}]} [log]
```

### 構文の説明

|                                   |  |
|-----------------------------------|--|
| <b>request</b>                    | (任意) ARP 要求との一致を定義します。 <b>request</b> 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。 |
| <b>ip</b>                         | 送信元 IP アドレスを指定します。   |
| <b>any</b>                        | IP アドレスまたは MAC アドレスを拒否します。   |
| <b>host sender-ip</b>             | 指定された送信側 IP アドレスを拒否します。  |
| <b>sender-ip sender-ip-mask</b>   | 指定された範囲の送信側 IP アドレスを許可します。   |
| <b>mac</b>                        | 送信側 MAC アドレスを拒否します。  |
| <b>host sender-mac</b>            | 特定の送信側 MAC アドレスを拒否します。   |
| <b>sender-mac sender-mac-mask</b> | 指定された範囲の送信側 MAC アドレスを拒否します。  |
| <b>response ip</b>                | ARP 応答の IP アドレス値を定義します。  |
| <b>host target-ip</b>             | 指定されたターゲット IP アドレスを拒否します。  |
| <b>target-ip target-ip-mask</b>   | 指定された範囲のターゲット IP アドレスを拒否します。   |
| <b>mac</b>                        | ARP 応答の MAC アドレス値を拒否します。   |
| <b>host target-mac</b>            | 指定されたターゲット MAC アドレスを拒否します。   |
| <b>target-mac target-mac-mask</b> | 指定された範囲のターゲット MAC アドレスを拒否します。  |
| <b>log</b>                        | (任意) ACE と一致するパケットを記録します。  |

### コマンド デフォルト

ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。

### コマンド モード

ARP アクセス リスト コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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。

## deny (ARP アクセス リスト コンフィギュレーション)

## 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  |
|---|---|
| <a href="#">arp access-list</a>                   | ARP アクセス コントロール リスト (ACL) を定義します。             |
| <a href="#">ip arp inspection filter vlan</a>     | 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。 |
| <a href="#">permit (ARP アクセス リスト コンフィギュレーション)</a> | 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。         |
| <a href="#">show arp access-list</a>              | ARP アクセス リストに関する詳細を表示します。                     |

## deny (MAC アクセス リスト コンフィギュレーション)

条件が一致した場合に、非 IP トラフィックの転送を回避するには、MAC 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。拒否条件を名前付き MAC アクセス リストから削除するには、このコマンドの **no** 形式を使用します。

```
{deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | cos cos | dec-spanning | decnet-iv | diagnostic
| dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console | mop-dump |
msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```

```
no {deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | cos cos | dec-spanning | decnet-iv | diagnostic
| dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console | mop-dump |
msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```

### 構文の説明

|  |   |
|--|---|
| <b>any</b>                                   | 送信元または宛先 MAC アドレスを拒否します。  |
| <b>host src MAC-addr   src-MAC-addr mask</b> | 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。  |
| <b>host dst-MAC-addr   dst-MAC-addr mask</b> | 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。   |
| <b>type mask</b>                             | (任意) Ethernet II または SNAP カプセル化によるパケットの Ethertype 番号を使用して、パケットのプロトコルを識別します。<br><br><i>type</i> には、0 ~ 65535 の 16 進数を指定できます。<br><br><i>mask</i> は、一致をテストする前に Ethertype に適用される <i>don't care</i> ビットのマスクです。 |
| <b>aarp</b>                                  | (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。  |
| <b>amber</b>                                 | (任意) EtherType DEC-Amber を選択します。  |
| <b>cos cos</b>                               | (任意) プライオリティを設定するため、0 ~ 7 までのサービス クラス (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。 <b>cos</b> 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。  |
| <b>dec-spanning</b>                          | (任意) EtherType Digital Equipment Corporation (DEC) スパニング ツリーを選択します。   |
| <b>decnet-iv</b>                             | (任意) EtherType DECnet Phase IV プロトコルを選択します。   |
| <b>diagnostic</b>                            | (任意) EtherType DEC-Diagnostic を選択します。   |
| <b>dsm</b>                                   | (任意) EtherType DEC-DSM を選択します。  |
| <b>etype-6000</b>                            | (任意) EtherType 0x6000 を選択します。   |
| <b>etype-8042</b>                            | (任意) EtherType 0x8042 を選択します。   |
| <b>lat</b>                                   | (任意) EtherType DEC-LAT を選択します。  |
| <b>lavc-sca</b>                              | (任意) EtherType DEC-LAVC-SCA を選択します。   |
| <b>lsap lsap-number mask</b>                 | (任意) 802.2 カプセル化によるパケットの LSAP 番号 (0 ~ 65535) を指定して、パケットのプロトコルを識別します。<br><br><i>mask</i> は、一致をテストする前に LSAP 番号に適用される <i>don't care</i> ビットのマスクです。   |

## deny (MAC アクセス リスト コンフィギュレーション)

|                    |   |
|--------------------|---|
| <b>mop-console</b> | (任意) EtherType DEC-MOP Remote Console を選択します。   |
| <b>mop-dump</b>    | (任意) EtherType DEC-MOP Dump を選択します。   |
| <b>msdos</b>       | (任意) EtherType DEC-MSDOS を選択します。  |
| <b>mumps</b>       | (任意) EtherType DEC-MUMPS を選択します。  |
| <b>netbios</b>     | (任意) EtherType DEC-Network Basic Input/Output System (NETBIOS) を選択します。  |
| <b>vines-echo</b>  | (任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) Echo を選択します。                       |
| <b>vines-ip</b>    | (任意) EtherType VINES IP を選択します。   |
| <b>xns-idp</b>     | (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 2-5 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 2-5 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  | Novel 名        |                  |
| arpa         | Ethernet II    | Ethertype 0x8137 |
| snap         | Ethernet-snap  | Ethertype 0x8137 |
| sap          | Ethernet 802.2 | LSAP 0xE0E0      |
| novell-ether | Ethernet 802.3 | LSAP 0xFFFF      |

## コマンド デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルトアクションは拒否です。

## コマンド モード

MAC アクセス リスト コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**mac access-list extended** グローバル コンフィギュレーション コマンドを使用して、MAC アクセス リスト コンフィギュレーション モードを開始します。

**host** キーワードを使用した場合、アドレス マスクは入力できません。**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。

アクセス コントロール エントリ (ACE) がアクセス コントロール リストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

名前付き MAC 拡張アクセス リストの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

**例**

次の例では、すべての送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを拒否する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは拒否されます。

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

次の例では、名前付き MAC 拡張アクセス リストから拒否条件を削除する方法を示します。

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

次の例では、EtherType 0x4321 のすべてのパケットを拒否します。

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

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

**関連コマンド**

| コマンド  | 説明   |
|---|--|
| <a href="#">mac access-list extended</a>          | 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。 |
| <a href="#">permit (MAC アクセス リスト コンフィギュレーション)</a> | 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。        |
| <a href="#">show access-lists</a>                 | スイッチに設定されたアクセス コントロール リストを表示します。           |

# dot1x

IEEE 802.1x 認証をグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで **dot1x** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x {critical {eapol | recovery delay milliseconds} | {guest-vlan supplicant} |
system-auth-control}
```

```
no dot1x {critical {eapol | recovery delay} | {guest-vlan supplicant} | system-auth-control}
```



(注)

**credentials name** キーワードは、コマンドラインのヘルプ スtring には表示されますが、サポートされていません。

## 構文の説明

|  |  |
|--|--|
| <b>critical {eapol   recovery delay <i>milliseconds</i>}</b> | アクセス不能認証バイパス パラメータを設定します。詳細については、 <b>dot1x critical (グローバル コンフィギュレーション)</b> コマンドを参照してください。 |
| <b>guest-vlan supplicant</b>                                 | スイッチでオプションのゲスト VLAN の動作をグローバルにイネーブルにします。   |
| <b>system-auth-control</b>                                   | スイッチで IEEE 802.1x 認証をグローバルにイネーブルにします。  |

## コマンド デフォルト

IEEE 802.1x 認証はディセーブルで、オプションのゲスト VLAN の動作はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

IEEE 802.1x 認証をグローバルにイネーブルにする前に、認証、許可、アカウントティング (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。方式リストには、ユーザの認証に使用する、順序と認証方式が記述されています。

スイッチの IEEE 802.1x 認証をグローバルにイネーブルにする前に、IEEE 802.1x 認証および EtherChannel が設定されているインターフェイスから EtherChannel の設定を削除します。

EAP-Transparent LAN Service (TLS) および EAP-MD5 で IEEE 802.1x を認証する Cisco Access Control Server (ACS) アプリケーションが稼働する装置を使用している場合、装置が ACS バージョン 3.2.1 以上で稼働していることを確認します。

**guest-vlan supplicant** キーワードを使用して、スイッチでオプションの IEEE 802.1x ゲスト VLAN の動作をグローバルにイネーブルにできます。詳細については、**dot1x guest-vlan** コマンドを参照してください。

**例** 次の例では、スイッチで IEEE 802.1x 認証をグローバルにイネーブルにする方法を示します。

```
Switch(config)# dot1x system-auth-control
```

次の例では、スイッチでオプションのゲスト VLAN の動作をグローバルにイネーブルにする方法を示します。

```
Switch(config)# dot1x guest-vlan supplicant
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

#### 関連コマンド

| コマンド   | 説明   |
|--|--|
| <b>dot1x critical</b> (グローバル<br>コンフィギュレーション)   | スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。                |
| <b>dot1x guest-vlan</b>                        | アクティブ VLAN をイネーブルにし、IEEE 802.1x ゲスト VLAN として指定します。 |
| <b>dot1x port-control</b>                      | 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。                        |
| <b>show dot1x [interface<br/>interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。                   |

# dot1x auth-fail max-attempts

ポートが制限 VLAN に移行するまでに許容できる最大認証試行回数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x auth-fail max-attempts** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x auth-fail max-attempts** *max-attempts*

**no dot1x auth-fail max-attempts**

## 構文の説明

*max-attempts* ポートが制限 VLAN に移行するまでに許容される最大認証試行回数を指定します。指定できる範囲は 1 ～ 3 です。デフォルト値は 3 です。

## コマンドデフォルト

デフォルト値は 3 回です。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

VLAN で許容される最大の認証試行回数を再設定する場合、変更内容は再認証タイマーが期限切れになった後で反映されます。

## 例

次の例では、ポート 3 の制限 VLAN にポートが移行する前に許容される最大の認証試行回数を 2 に設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド   | 説明  |
|--|---|
| <code>dot1x auth-fail vlan [vlan id]</code>      | オプションの制限 VLAN の機能をイネーブルにします。                  |
| <code>dot1x max-reauth-req [count]</code>        | ポートが無許可状態に移行する前に、スイッチが認証プロセスを再起動する最大回数を設定します。 |
| <code>show dot1x [interface interface-id]</code> | 指定されたポートの IEEE 802.1x の状態を表示します。              |

## dot1x auth-fail vlan

ポートで制限 VLAN をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x auth-fail vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x auth-fail vlan vlan-id
```

```
no dot1x auth-fail vlan
```

### 構文の説明

*vlan-id* VLAN を 1 ~ 4094 の範囲で指定します。

### コマンドデフォルト

制限 VLAN は設定されていません。

### コマンドモード

インターフェイス コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

次のように設定されたポートで制限 VLAN を設定できます。

- シングルホスト (デフォルト) モード
- 認証用 auto モード

再認証をイネーブルにする必要があります。ディセーブルになっていると、制限 VLAN のポートは再認証要求を受け取りません。再認証プロセスを開始するには、制限 VLAN がポートからリンクダウン イベントまたは Extensible Authentication Protocol (EAP) ログオフ イベントを受け取る必要があります。ホストがハブを介して接続されている場合、ホストが切断されているとポートがリンクダウン イベントを受け取ることができず、次の再認証試行が行われるまで新しいホストが検出されないことがあります。

サブリカントが認証に失敗すると、ポートは制限 VLAN に移行し、EAP 認証成功メッセージがサブリカントに送信されます。サブリカントには実際の認証失敗が通知されないため、この制限ネットワークアクセスに混乱が生じることがあります。EAP の成功メッセージは、次の理由で送信されます。

- EAP の成功メッセージが送信されない場合、サブリカントは 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。

サブリカントは、認証から EAP 成功メッセージを受け取った後で不正なユーザ名とパスワードの組み合わせをキャッシュし、再認証のたびにその情報を使用する可能性があります。サブリカントが正しいユーザ名とパスワードの組み合わせを送信するまで、ポートは制限 VLAN のままになります。

レイヤ 3 ポートに使用する内部 VLAN は、制限 VLAN として設定することはできません。

VLAN を制限 VLAN と音声 VLAN の両方に設定することはできません。そのように設定すると、syslog メッセージが生成されます。

制限 VLAN ポートが無許可ステートに移行すると、認証プロセスが再起動されます。サブリカントが再度認証プロセスに失敗すると、認証は保持ステートで待機します。サブリカントが正常に再認証された後、すべての IEEE 802.1x ポートが再初期化され、通常の IEEE 802.1x ポートとして扱われます。

制限 VLAN を異なる VLAN として再設定すると、制限 VLAN のポートも移行し、そのポートは現在認証されたステートのままになります。

制限 VLAN をシャットダウンするか VLAN データベースから削除すると、制限 VLAN のポートはただちに無許可ステートに移行し、認証プロセスが再起動します。制限 VLAN 設定がまだ存在するため、認証は保持ステートで待機しません。制限 VLAN が非アクティブである間も、制限 VLAN がアクティブになったときにポートがただちに制限 VLAN になるように、すべての認証試行がカウントされます。

制限 VLAN は、シングルホスト モード（デフォルトのポート モード）でだけサポートされます。そのため、ポートが制限 VLAN に配置されると、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、ポートに表示される他の MAC アドレスは、すべてセキュリティ違反として扱われます。

## 例

次の例では、ポート 1 で制限 VLAN を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

設定を確認するには、`show dot1x [interface interface-id]` 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド   | 説明                                       |
|--|--|
| <code>dot1x auth-fail max-attempts [max-attempts]</code> | サブリカントを制限 VLAN に割り当てる前に、試行可能な認証回数を設定します。 |
| <code>show dot1x [interface interface-id]</code>         | 指定されたポートの IEEE 802.1x の状態を表示します。         |

# dot1x control-direction

wake-on-LAN (WoL) 機能を搭載した IEEE 802.1x 認証をイネーブルにし、ポート制御を単一方モードまたは双方向モードに設定するには、インターフェイス コンフィギュレーション モードで **dot1x control-direction** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x control-direction {both | in}**

**no dot1x control-direction**

## 構文の説明

|             |   |
|-------------|---|
| <b>both</b> | 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。         |
| <b>in</b>   | ポートの単一方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。 |

## コマンド デフォルト

ポートは双方向モードに設定されています。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

WoL の詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication (IEEE 802.1x ポートベース認証の設定)」の章の「Using IEEE 802.1x Authentication with Wake-on-LAN (Wake-on-LAN を使った IEEE 802.1x 認証の使用)」の項を参照してください。

## 例

次の例では、単一方制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction in
```

次の例では、双方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction both
```

設定を確認するには、**show dot1x all** 特権 EXEC コマンドを入力します。

**show dot1x all** 特権 EXEC コマンド出力は、ポート名とポートの状態を除き、すべてのスイッチで同一です。ホストがポートに接続されていてまだ認証されていない場合、次のように表示されます。

```
Supplicant MAC 0002.b39a.9275
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
```

**dot1x control-direction in** インターフェイス コンフィギュレーション コマンドを入力して単一方向制御をイネーブルにする場合、これが **show dot1x all** コマンド出力で次のように表示されます。

```
ControlDirection = In
```

**dot1x control-direction in** インターフェイス コンフィギュレーション コマンドを入力しても、設定の競合によりポートでこのモードをサポートできない場合、**show dot1x all** コマンド出力で次のように表示されます。

```
ControlDirection = In (Disabled due to port settings)
```

#### 関連コマンド

| コマンド   | 説明                                     |
|--|--|
| <b>show dot1x</b> [ <b>all</b>   <b>interface interface-id</b> ] | 指定したインターフェイスに対する制御方向のポート設定ステータスを表示します。 |

# dot1x credentials (グローバル コンフィギュレーション)

サブリカント スイッチでプロファイルを設定するには、グローバル コンフィギュレーション モードで **dot1x credentials** コマンドを使用します。

**dot1x credentials profile**

**no dot1x credentials profile**

|       |                |                           |
|-------|----------------|---------------------------|
| 構文の説明 | <i>profile</i> | サブリカント スイッチのプロファイルを指定します。 |
|-------|----------------|---------------------------|

|            |                      |
|------------|----------------------|
| コマンド デフォルト | スイッチにプロファイルは設定されません。 |
|------------|----------------------|

|          |                   |
|----------|-------------------|
| コマンド モード | グローバル コンフィギュレーション |
|----------|-------------------|

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

|            |  |
|------------|--|
| 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。<br>Switch(config)# <b>dot1x credentials profile</b><br><br>設定を確認するには、 <b>show running-config</b> 特権 EXEC コマンドを入力します。 |
|---|---|

| 関連コマンド | コマンド               | 説明  |
|--------|--------------------|---|
|        | <b>cisp enable</b> | Client Information Signalling Protocol (CISP) をイネーブルにします。 |
|        | <b>show cisp</b>   | 指定されたインターフェイスの CISP 情報を表示します。                             |

## dot1x critical (グローバル コンフィギュレーション)

クリティカル認証または認証、許可、アカウントिंग (AAA) 失敗ポリシーとも呼ばれているアクセス不能な認証バイパス機能のパラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x critical {eapol | recovery delay milliseconds}
```

```
no dot1x critical {eapol | recovery delay}
```

### 構文の説明

|                                    |   |
|------------------------------------|---|
| <b>eapol</b>                       | スイッチによりクリティカルなポートが <b>critical-authentication</b> ステートに置かれた場合、EAPOL-Success メッセージを送信するようスイッチを指定します。 |
| <b>recovery delay milliseconds</b> | ミリ秒のリカバリ遅延のペリオドを設定します。指定できる範囲は 1 ~ 10000 ミリ秒です。   |

### コマンド デフォルト

クリティカルなポートを **critical-authentication** ステートに置くことによってそのクリティカルなポートの認証に成功した場合に、スイッチは EAPOL-Success メッセージをホストに送信しません。リカバリ遅延期間は、1000 ミリ秒 (1 秒) です。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

クリティカルなポートが **critical-authentication** ステートに置かれた場合、スイッチが EAPOL-Success メッセージを送信するよう指定するには、**eapol** キーワードを使用します。

使用不能な RADIUS サーバが使用可能になった場合にスイッチがクリティカルなポートを再初期化するために待機するリカバリ遅延期間を設定するには、**recovery delay milliseconds** キーワードを使用します。デフォルトのリカバリ遅延期間は 1000 ミリ秒です。ポートは、秒単位で再初期化できます。

アクセス不能な認証バイパスをポート上でイネーブルにするには、**dot1x critical** インターフェイス コンフィギュレーション コマンドを使用します。スイッチがクリティカルなポートに割り当てるアクセス VLAN を設定するには、**dot1x critical vlan vlan-id** インターフェイス コンフィギュレーション コマンドを使用します。

### 例

次の例では、リカバリ遅延期間として 200 をスイッチに設定する方法を示します。

```
Switch# dot1x critical recovery delay 200
```

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

## ■ dot1x critical (グローバル コンフィギュレーション)

| 関連コマンド | コマンド  | 説明   |
|--------|---|--|
|        | <a href="#">dot1x critical (インターフェイス コンフィギュレーション)</a> | アクセス不能な認証バイパス機能をイネーブルにし、この機能にアクセス VLAN を設定します。 |
|        | <a href="#">show dot1x</a>                            | 指定されたポートの IEEE 802.1x の状態を表示します。               |

# dot1x critical (インターフェイス コンフィギュレーション)

クリティカル認証または認証、許可、アカウントिंग (AAA) 失敗ポリシーとも呼ばれているアクセス不能な認証バイパス機能のパラメータをイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x critical** コマンドを使用します。ポートが **critical-authentication** ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定することもできます。この機能をディセーブルにするか、またはデフォルトに戻すには、このコマンドの **no** 形式を使用します。

```
dot1x critical [recovery action reinitialize | vlan vlan-id]
```

```
no dot1x critical [recovery | vlan]
```

## 構文の説明

|                                     |  |
|-------------------------------------|--|
| <b>recovery action reinitialize</b> | (任意) アクセス不能な認証バイパスのリカバリ機能をイネーブルにし、認証サーバが使用可能になった場合にリカバリ アクションによりポートを認証するよう指定します。 |
| <b>vlan <i>vlan-id</i></b>          | (任意) スイッチがクリティカルなポートに割り当てることができるアクセス VLAN を指定します。有効な範囲は 1 ~ 4094 です。             |

## コマンド デフォルト

アクセス不能認証バイパス機能はディセーブルです。  
リカバリ アクションは設定されていません。  
アクセス VLAN は設定されていません。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

ポートが **critical-authentication** ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を指定するには、**vlan *vlan-id*** キーワードを使用します。指定された VLAN タイプは、次のようにポートタイプに適合している必要があります。

- クリティカルなポートがアクセス ポートの場合、VLAN はアクセス VLAN でなければなりません。
- クリティカルなポートがルーテッド ポートの場合、VLAN を指定できます (指定は任意)。

クライアントで Windows XP を稼働し、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 クライアントが DHCP 用に設定されていて、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP-Success メッセージを受信しても DHCP 設定プロセスが再開されない場合があります。

## ■ dot1x critical (インターフェイス コンフィギュレーション)

アクセス不能認証バイパス機能および制限 VLAN を IEEE802.1x ポート上に設定できます。スイッチが制限 VLAN でクリティカル ポートの再認証を試行し、RADIUS サーバがすべて使用できない場合、スイッチはポートの状態をクリティカル認証ステートに移行し、ポートは制限 VLAN のままとなります。

アクセス不能認証バイパス機能とポート セキュリティは、同じスイッチ ポートに設定できます。

## 例

次の例では、アクセス不能認証バイパス機能をポート上でイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x critical
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                       | 説明                                  |
|--|-------------------------------------|
| <b>dot1x critical</b> (グローバル コンフィギュレーション)  | スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。 |
| <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。    |

# dot1x default

デフォルト値に IEEE 802.1x パラメータをリセットするには、インターフェイス コンフィギュレーション モードで **dot1x default** 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。

### コマンド 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)。
- 再認証試行間隔の秒数は、3600 秒です。
- 定期的な再認証はディセーブルです。
- 待機時間は 60 秒です。
- 再伝送時間は 30 秒です。
- 最高再伝送回数は 2 回です。
- ホスト モードはシングル ホストです。
- クライアントのタイムアウト時間は 30 秒です。
- 認証サーバのタイムアウト時間は 30 秒です。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 例

次の例では、ポート上の IEEE 802.1x パラメータをリセットする方法を示します。

```
Switch(config-if)# dot1x default
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

### 関連コマンド

| コマンド                                       | 説明                               |
|--|----------------------------------|
| <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。 |

# dot1x fallback

ポートを 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に設定するには、インターフェイス コンフィギュレーション モードで **dot1xfallback** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x fallback profile**

**no dot1x fallback**

## 構文の説明

|                |  |
|----------------|--|
| <i>profile</i> | IEEE 802.1x 認証をサポートしていないクライアントのフォールバック プロファイル。 |
|----------------|--|

## コマンドデフォルト

フォールバックはイネーブルではありません。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドを入力する前に、スイッチ ポートで **dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

## 例

次の例では、IEEE 802.1x 認証用に設定されているスイッチ ポートにフォールバック プロファイルを指定する方法を示します。

```
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド  | 説明                               |
|---|----------------------------------|
| <a href="#">fallback profile</a>                    | Web 認証のフォールバック プロファイルを作成します。     |
| <a href="#">ip admission</a>                        | ポートの Web 認証をイネーブルにします。           |
| <a href="#">ip admission name proxy http</a>        | スイッチの Web 認証をグローバルにイネーブルにします。    |
| <a href="#">show dot1x [interface interface-id]</a> | 指定されたポートの IEEE 802.1x の状態を表示します。 |

# dot1x guest-vlan

アクティブ VLAN を IEEE 802.1x ゲスト VLAN として指定するには、インターフェイス コンフィギュレーション モードで **dot1x guest-vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x guest-vlan vlan-id
```

```
no dot1x guest-vlan
```

## 構文の説明

|                |  |
|----------------|--|
| <i>vlan-id</i> | IEEE 802.1x ゲスト VLAN であるアクティブ VLAN。指定できる範囲は 1 ～ 4094 です。 |
|----------------|--|

## コマンドデフォルト

ゲスト VLAN は設定されません。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

非プライベート VLAN に属するスタティック アクセス ポートにゲスト VLAN を設定できます。

スイッチの IEEE 802.1x ポートごとにゲスト VLAN を設定して、現在 IEEE 802.1x 認証を実行していないクライアント（スイッチに接続されているデバイスまたはワークステーション）へのサービスを制限できます。こうしたユーザは IEEE 802.1x 認証のためにシステムをアップグレードできますが、Windows 98 システムなどのホストでは IEEE 802.1x に対応できません。

IEEE 802.1x ポートでゲスト VLAN をイネーブルにした場合、認証サーバが Extensible Authentication Protocol over LAN (EAPOL) Request/Identity フレームに対する応答を受信しない、あるいは EAPOL パケットがクライアントから送信されないと、スイッチではクライアントをゲスト VLAN に割り当てます。

スイッチは EAPOL パケット履歴を保持します。リンクの存続時間内に別の EAPOL パケットがインターフェイス上で検出された場合、ゲスト VLAN 機能はディセーブルになります。ポートがすでにゲスト VLAN ステートにある場合、ポートは無許可ステートに戻り、認証が再開されます。EAPOL 履歴はリンクの損失でリセットされます。

スイッチ ポートがゲスト VLAN に移行すると、IEEE 802.1x 非対応クライアントはいくつでもアクセスが許可されます。IEEE 802.1x 対応クライアントが、ゲスト VLAN を設定しているポートと同じポートに加入すると、ポートは RADIUS 設定 VLAN またはユーザ設定アクセス VLAN では無許可ステートに移行し、認証が再開されます。

ゲスト VLAN は、シングルホスト モードおよびマルチホスト モードの IEEE 802.1x ポート上でサポートされます。

リモートスイッチド ポート アナライザ (RSPAN) VLAN、音声 VLAN 以外のアクティブなすべての VLAN は、IEEE 802.1x ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN (ルーテッドポート) またはトランク ポート上ではサポートされません。サポートされるのはアクセスポートだけです。

DHCP クライアントが接続されている IEEE 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり、DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の IEEE 802.1x 認証プロセスを再起動する設定を変更できます。IEEE 802.1x 認証プロセスの設定を減らします (**dot1x timeout quiet-period** および **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンド)。設定の減少量は、接続された IEEE 802.1x クライアントのタイプによって異なります。

スイッチは *MAC 認証バイパス* をサポートします。MAC 認証バイパスは IEEE 802.1x ポートでイネーブルの場合、スイッチは、EAPOL メッセージ交換を待機している間に IEEE802.1x 認証が期限切れになると、クライアントの MAC アドレスに基づいてクライアントを許可できます。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ

RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます (指定されていない場合)。詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication (IEEE 802.1x ポートベース認証の設定)」の章の「Using IEEE 802.1x Authentication with MAC Authentication Bypass (MAC 認証バイパスを使った IEEE 802.1x 認証の使用)」の項を参照してください。

**例**

次の例では、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config-if)# dot1x guest-vlan 5
```

次の例では、スイッチの待機時間を 3 秒に設定し、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を 15 に設定する方法、および IEEE 802.1x ポートが DHCP クライアントに接続されているときに VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする方法を示します。

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

次の例では、オプションのゲスト VLAN の動作をイネーブルにし、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x guest-vlan 5
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

**関連コマンド**

| コマンド                                       | 説明                                  |
|--|-------------------------------------|
| <b>dot1x</b>                               | オプションのゲスト VLAN のサブリカント機能をイネーブルにします。 |
| <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。    |

# dot1x host-mode

IEEE 802.1x 許可ポートで単一のホスト（クライアント）または複数のホストを許可するには、インターフェイス コンフィギュレーション モードで **dot1x host-mode** コマンドを使用します。IEEE 802.1x 許可ポートでマルチドメイン認証（MDA）をイネーブルにするには、**multi-domain** キーワードを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x host-mode {multi-host | single-host | multi-domain}
```

```
no dot1x host-mode [multi-host | single-host | multi-domain]
```

## 構文の説明

|                     |                            |
|---------------------|----------------------------|
| <b>multi-host</b>   | スイッチ上で複数のホストをイネーブルにします。    |
| <b>single-host</b>  | スイッチ上で単一のホストをイネーブルにします。    |
| <b>multi-domain</b> | スイッチ ポート上で MDA をイネーブルにします。 |

## コマンド デフォルト

デフォルト設定は、シングルホスト モードです。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドを使用すると、IEEE 802.1x 対応ポートを単一のクライアントに限定したり、複数のクライアントを IEEE 802.1x 対応ポートに接続したりすることができます。マルチホスト モードでは、接続されたホストのうち 1 つだけが許可されれば、すべてのホストのネットワーク アクセスが許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、または Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

ポートで MDA をイネーブルにするには、**multi-domain** キーワードを使用します。MDA はポートをデータ ドメインと音声ドメインの両方に分割します。MDA により、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が同じ IEEE 802.1x 対応ポート上で許可されます。

このコマンドを入力する前に、指定のポートで **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認します。

## 例

次の例では、IEEE 802.1x 認証をグローバルにイネーブルにして、ポートの IEEE 802.1x 認証をイネーブルにし、マルチホスト モードをイネーブルにする方法を示します。

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

次の例では、IEEE 802.1x 認証をグローバルにイネーブルにし、IEEE 802.1x 認証をイネーブルにし、指定されたポートで MDA をイネーブルにする方法を示します。

```
Switch(config)# dot1x system-auth-control
```

## ■ dot1x host-mode

```
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                       | 説明                               |
|--|----------------------------------|
| <b>show dot1x [interface interface-id]</b> | 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状態に戻すには、特権 EXEC モードで **dot1x initialize** コマンドを使用します。

**dot1x initialize [interface interface-id]**

| 構文の説明                                      | <b>interface interface-id</b> (任意) 初期化するポートを指定します。  |      |      |  |                                  |
|--|---|------|------|--|----------------------------------|
| コマンド デフォルト                                 | なし  |      |      |  |                                  |
| コマンド モード                                   | 特権 EXEC   |      |      |  |                                  |
| コマンド履歴                                     | <table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>15.0(1)EY</td><td>このコマンドが導入されました。</td></tr></tbody></table>   | リリース | 変更内容 | 15.0(1)EY                                  | このコマンドが導入されました。                  |
| リリース                                       | 変更内容  |      |      |  |                                  |
| 15.0(1)EY                                  | このコマンドが導入されました。   |      |      |  |                                  |
| 使用上のガイドライン                                 | このコマンドは、IEEE 802.1x ステート マシンを初期化し、新たな認証環境を設定します。このコマンドを入力した後、ポートの状態は無許可になります。   |      |      |  |                                  |
| 例  | 次の例では、ポートを手動で初期化する方法を示します。<br><pre>Switch# dot1x initialize interface gigabitethernet1/2</pre><br><b>show dot1x [interface interface-id]</b> 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                                     | <table><thead><tr><th>コマンド</th><th>説明</th></tr></thead><tbody><tr><td><b>show dot1x [interface interface-id]</b></td><td>指定されたポートの IEEE 802.1x の状態を表示します。</td></tr></tbody></table>               | コマンド | 説明   | <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。 |
| コマンド                                       | 説明  |      |      |  |                                  |
| <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。  |      |      |  |                                  |

# dot1x mac-auth-bypass

MAC 認証バイパス機能をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x mac-auth-bypass** コマンドを使用します。MAC 認証バイパス機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
dot1x mac-auth-bypass [eap | timeout inactivity value]
```

```
no dot1x mac-auth-bypass
```

## 構文の説明

|                                 |  |
|---------------------------------|--|
| <b>eap</b>                      | (任意) 認証に Extensible Authentication Protocol (EAP) を使用するようスイッチを設定します。 |
| <b>timeout inactivity value</b> | (任意) 接続されたホストが無許可ステートになる前に非アクティブである秒数を設定します。指定できる範囲は 1 ~ 65535 です。   |

## コマンド デフォルト

MAC 認証バイパスはディセーブルです。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

特に言及されない限り、MAC 認証バイパス機能の使用上のガイドラインは IEEE802.1x 認証の使用上のガイドラインと同じです。

ポートが MAC アドレスで認証された後で、ポートから MAC 認証バイパス機能をディセーブルにした場合、ポート ステートには影響ありません。

ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバデータベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加された場合、スイッチは MAC 認証バイパスを使用してポートを再許可できます。

ポートが許可ステートの場合、再許可が発生するまでポートはこのステートのままになります。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが IEEE 802.1x 対応サブリカントであることを確認し、(MAC 認証バイパス機能ではなく) IEEE 802.1x 認証を使用してインターフェイスを認証します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。

MAC 認証バイパスおよび IEEE 802.1x 認証の相互作用の詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication (IEEE 802.1x ポートベース認証の設定)」の章の「Understanding IEEE 802.1x Authentication with MAC Authentication Bypass (MAC 認証バイパスを使った IEEE 802.1x 認証について)」の項および「IEEE 802.1x Authentication Configuration Guidelines (IEEE 802.1x 認証設定ガイドライン)」の項を参照してください。

## 例

次の例では、MAC 認証バイパスをイネーブルにし、認証に EAP を使用するようスイッチを設定する方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass eap
```

次の例では、MAC 認証バイパスをイネーブルにし、接続されたホストが 30 秒間非アクティブである場合にタイムアウトを設定する方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass timeout inactivity 30
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

#### 関連コマンド

| コマンド   | 説明                               |
|--|----------------------------------|
| <code>show dot1x [interface interface-id]</code> | 指定されたポートの IEEE 802.1x の状態を表示します。 |

# dot1x max-reauth-req

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再起動する回数の最大数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x max-reauth-req** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x max-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、スイッチが認証プロセスを再起動する回数です。指定できる範囲は 0 ~ 10 です。 |
|--------------|--|

## コマンドデフォルト

デフォルトは 2 回です。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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   |
|--|--|
| <b>dot1x max-req</b>                       | 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)。       |
| <b>dot1x timeout tx-period</b>             | 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。 |
| <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。                                       |

# dot1x max-req

認証プロセスを再開する前に、スイッチが Extensible Authentication Protocol (EAP) フレーム（応答が受信されないと見なされます）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、インターフェイス コンフィギュレーション モードで **dot1x max-req** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x max-req count
```

```
no dot1x max-req
```

|       |              |  |
|-------|--------------|--|
| 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、認証サーバから EAP フレームを再送信する回数です。範囲は 1 ~ 10 です。 |
|-------|--------------|--|

コマンド デフォルト

デフォルトは 2 回です。

コマンド モード

インターフェイス コンフィギュレーション

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

例

次の例では、認証プロセスを再起動する前に、スイッチが EAP フレームを認証サーバからクライアントに送信する回数を 5 回に設定する方法を示します。

```
Switch(config-if)# dot1x max-req 5
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

| 関連コマンド | コマンド                                       | 説明   |
|--------|--|--|
|        | <b>dot1x timeout tx-period</b>             | 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。 |
|        | <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。                                       |

# dot1x pae

IEEE 802.1x Port Access Entity (PAE) オーセンティケータとしてポートを設定するには、インターフェイス コンフィギュレーション モードで **dot1x pae** コマンドを使用します。IEEE 802.1x 認証をポート上でディセーブルにするには、このコマンドの **no** 形式を使用します。

**dot1x pae authenticator**

**no dot1x pae**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

ポートは IEEE 802.1x PAE オーセンティケータではありません。IEEE 802.1x 認証はポート上でディセーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

IEEE 802.1x 認証をポート上でディセーブルにする場合は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

**dot1x port-control** インターフェイス コンフィギュレーション コマンドを入力するなどしてポート上で IEEE 802.1x 認証を設定した場合、スイッチは自動的にポートを IEEE 802.1x オーセンティケータとして設定します。オーセンティケータの PAE 動作は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを入力した後でディセーブルになります。

## 例

次の例では、ポートの IEEE 802.1x 認証をディセーブルにする方法を示します。

```
Switch(config-if)# no dot1x pae
```

設定を確認するには、**show dot1x** または **show eap** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                       | 説明  |
|----------------------------|---|
| <a href="#">show dot1x</a> | 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。 |
| <a href="#">show eap</a>   | スイッチまたは指定されたポートの EAP のレジストレーション情報およびセッション情報を表示します。          |

# dot1x port-control

ポートの認証ステータスの手動制御をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x port-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x port-control {auto | force-authorized | force-unauthorized}
```

```
no dot1x port-control
```

## 構文の説明

|                           |   |
|---------------------------|---|
| <b>auto</b>               | ポートで IEEE 802.1x 認証をイネーブルにし、スイッチおよびクライアント間の IEEE 802.1x 認証交換に基づきポートを許可または無許可ステータスに変更します。                        |
| <b>force-authorized</b>   | ポートで IEEE 802.1x 認証をディセーブルにし、認証情報の交換をせずにポートを許可ステータスに移行します。ポートはクライアントとの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。 |
| <b>force-unauthorized</b> | クライアントからの認証の試みをすべて無視し、ポートを強制的に無許可ステータスに変更することにより、このポート経由のすべてのアクセスを拒否します。スイッチはポートを介してクライアントに認証サービスを提供できません。      |

## コマンド デフォルト

デフォルトの設定は **force-authorized** です。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

特定のポートの IEEE 802.1x 認証をイネーブルにする前に、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、スイッチの IEEE 802.1x 認証をグローバルにイネーブルにする必要があります。

IEEE 802.1x 標準は、レイヤ 2 のスタティック アクセス ポート、音声 VLAN のポート、およびレイヤ 3 のルーテッド ポート上でサポートされます。

ポートが、次の項目の 1 つとして設定されていない場合に限り **auto** キーワードを使用できます。

- **トランク ポート**：トランク ポートで IEEE 802.1x 認証をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
- **ダイナミック ポート**：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x 認証をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。

- ダイナミック アクセス ポート：ダイナミック アクセス (VLAN Query Protocol (VQP)) ポートで IEEE 802.1x 認証をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとする、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。
- スイッチド ポート アナライザ (SPAN) および Remote SPAN (RSPAN) 宛先ポート：SPAN または RSPAN 宛先ポートであるポートの IEEE 802.1x 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先として削除されるまで、IEEE 802.1x 認証はディセーブルのままです。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

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

**例**

次の例では、ポートの IEEE 802.1x 認証をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x port-control auto
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

**関連コマンド**

| コマンド                                       | 説明                               |
|--|----------------------------------|
| <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。 |

# dot1x re-authenticate

指定された IEEE 802.1x 対応ポートの再認証を手動で開始するには、特権 EXEC モードで **dot1x re-authenticate** コマンドを使用します。

```
dot1x re-authenticate [interface interface-id]
```

| 構文の説明                                       | <b>interface interface-id</b> (任意) 再認証するインターフェイスのモジュールおよびポート番号。   |      |      |  |                        |   |                    |
|---|---|------|------|--|------------------------|---|--------------------|
| コマンド デフォルト                                  | なし  |      |      |  |                        |   |                    |
| コマンド モード                                    | 特権 EXEC   |      |      |  |                        |   |                    |
| コマンド履歴                                      | <table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>15.0(1)EY</td><td>このコマンドが導入されました。</td></tr></tbody></table>   | リリース | 変更内容 | 15.0(1)EY                              | このコマンドが導入されました。        |   |                    |
| リリース  | 変更内容  |      |      |  |                        |   |                    |
| 15.0(1)EY                                   | このコマンドが導入されました。   |      |      |  |                        |   |                    |
| 使用上のガイドライン                                  | このコマンドを使用すると、再認証試行 (re-authperiod) と自動再認証の間に設定された期間 (秒) を待機することなく、クライアントを再認証できます。   |      |      |  |                        |   |                    |
| 例   | 次に、ポートに接続されたデバイスを手動で再認証する例を示します。<br>Switch# <b>dot1x re-authenticate interface gigabitethernet1/2</b>   |      |      |  |                        |   |                    |
| 関連コマンド                                      | <table><thead><tr><th>コマンド</th><th>説明</th></tr></thead><tbody><tr><td><a href="#">dot1x reauthentication</a></td><td>クライアントの定期的な再認証を有効にします。</td></tr><tr><td><a href="#">dot1x timeout reauth-period</a></td><td>再認証の間隔 (秒) を設定します。</td></tr></tbody></table> | コマンド | 説明   | <a href="#">dot1x reauthentication</a> | クライアントの定期的な再認証を有効にします。 | <a href="#">dot1x timeout reauth-period</a> | 再認証の間隔 (秒) を設定します。 |
| コマンド  | 説明  |      |      |  |                        |   |                    |
| <a href="#">dot1x reauthentication</a>      | クライアントの定期的な再認証を有効にします。  |      |      |  |                        |   |                    |
| <a href="#">dot1x timeout reauth-period</a> | 再認証の間隔 (秒) を設定します。  |      |      |  |                        |   |                    |

# dot1x reauthentication

クライアントの定期的な再認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x reauthentication** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**dot1x reauthentication**

**no dot1x reauthentication**

## 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

定期的な再認証はディセーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドを使用して、定期的な再認証を行う間隔の時間量を設定します。

## 例

次に、クライアントの定期的な再認証をディセーブルにする例を示します。

```
Switch(config-if)# no dot1x reauthentication
```

次に、定期的な再認証をイネーブルにし、再認証を試行する間隔を 4000 秒に設定する例を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                       | 説明                                    |
|--|---------------------------------------|
| <b>dot1x re-authenticate</b>               | すべての IEEE 802.1x 対応ポートの再認証を手動で初期化します。 |
| <b>dot1x timeout reauth-period</b>         | 再認証の間隔（秒）を設定します。                      |
| <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。      |

# 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、特権 EXEC モードで **dot1x test eapol-capable** 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) 照会されるポートを指定します。

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 gigabitethernet1/2
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/2 is EAPOL
capable
```

## 関連コマンド

| コマンド                                     | 説明  |
|--|---|
| <b>dot1x test timeout</b> <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、グローバル コンフィギュレーション モードで **dot1x test timeout** 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。 |
|----------------|---|

### コマンドデフォルト

デフォルト設定は 10 秒です。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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  |
|---|---|
| <b>dot1x test eapol-capable</b> [ <b>interface interface-id</b> ] | 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 タイマーを設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x timeout {quiet-period seconds | ratelimit-period seconds | reauth-period {seconds | server} | server-timeout seconds | supp-timeout seconds | tx-period seconds}
```

```
no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}
```

## 構文の説明

|   |  |
|---|--|
| <b>quiet-period seconds</b>             | 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を指定します。指定できる範囲は 1 ～ 65535 です。   |
| <b>ratelimit-period seconds</b>         | 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を指定します。指定できる範囲は 1 ～ 65535 です。   |
| <b>reauth-period {seconds   server}</b> | 再認証の間隔 (秒) を設定します。<br>キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>seconds</b> : 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。</li> <li><b>server</b> : 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。</li> </ul> |
| <b>server-timeout seconds</b>           | 認証サーバに対して、スイッチの packets 再送信を待機する秒数を指定します。指定できる範囲は 30 ～ 65535 です  |
| <b>supp-timeout seconds</b>             | 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を指定します。指定できる範囲は 30 ～ 65535 です   |
| <b>tx-period seconds</b>                | 要求を再送信するまでに、スイッチがクライアントからの EAP-Request/Identity フレームに対する応答を待機する秒数を指定します。指定できる範囲は 1 ～ 65535 です。   |

## コマンド デフォルト

デフォルトの設定は次のとおりです。

**reauth-period** は 3600 秒です。

**quiet-period** は 60 秒です。

**tx-period** は 5 秒です。

**supp-timeout** は 30 秒です。

**server-timeout** は 30 秒です。

**rate-limit** は 1 秒です。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにしただけの場合、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドは、スイッチの動作に影響します。

待機時間の間、スイッチはどのような認証要求も受け付けず、開始もしません。デフォルトよりも小さい数を入力することによって、ユーザへの応答時間を短縮できます。

**ratelimit-period** が 0 (デフォルト) に設定された場合、スイッチは認証に成功したクライアントからの EAPOL パケットを無視し、それらを RADIUS サーバに転送します。

## 例

次に、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する例を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

次に、定期的な再認証をイネーブルにし、再認証の間隔 (秒) としてセッション タイムアウト RADIUS 属性の値を指定する例を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

次の例では、スイッチの待機時間を 30 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

次の例では、スイッチから認証サーバへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config)# dot1x timeout server-timeout 45
```

次の例では、EAP request フレームに対するスイッチからクライアントへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout supp-timeout 45
```

次に、要求を再送信するまでに、クライアントからの EAP 要求 /ID フレームに対する応答を待機する秒数を 60 に設定する例を示します。

```
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   |
|-------------------------------|--|
| <b>dot1x max-req</b>          | 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。 |
| <b>dot1x reauthentication</b> | クライアントの定期的な再認証を有効にします。   |
| <b>show dot1x</b>             | すべてのポートの IEEE 802.1x ステータスを表示します。                              |

# dot1x violation-mode

新しいデバイスをポートに接続するか、最大数のデバイスをポートに接続した後で新しいデバイスをポートに接続するときに発生する違反モードを設定するには、インターフェイス コンフィギュレーション モードで **dot1x violation-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
dot1x violation-mode {shutdown | restrict | protect}
```

```
no dot1x violation-mode
```

## 構文の説明

|                 |  |
|-----------------|--|
| <b>shutdown</b> | エラーによって、予期しない新たな MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。 |
| <b>restrict</b> | 違反エラーの発生時に Syslog エラーを生成します。                           |
| <b>protect</b>  | 新しい MAC アドレスからパケットをそのままドロップします。これがデフォルト設定です。           |

## コマンド デフォルト

デフォルトでは、**dot1x violation-mode protect** がイネーブルになっています。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、新しいデバイスをポートに接続するときに、IEEE 802.1x 対応ポートを **errdisable** に設定して、シャットダウンする方法を示します。

```
Switch(config-if)# dot1x violation-mode shutdown
```

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

```
Switch(config-if)# dot1x violation-mode restrict
```

次の例では、新しいデバイスをポートに接続するときに、新たに接続されたデバイスを無視するように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# dot1x violation-mode protect
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                       | 説明                               |
|--|----------------------------------|
| <b>show dot1x [interface interface-id]</b> | 指定されたポートの IEEE 802.1x の状態を表示します。 |

# duplex

ポートのデュプレックスモードで動作するように指定するには、インターフェイス コンフィギュレーションモードで **duplex** 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

|             |  |
|-------------|--|
| <b>auto</b> | 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で動作すべきかを判断します）。                            |
| <b>full</b> | 全二重モードをイネーブルにします。  |
| <b>half</b> | 半二重モードをイネーブルにします（10 または 100 Mb/s で動作するインターフェイスに限る）。1000 または 10,000 Mb/s で動作するインターフェイスに対して半二重モードを設定できません。 |

## コマンドデフォルト

ファストイーサネットポートおよびギガビットイーサネットポートに対するデフォルトは **auto** です。100BASE-x（-x は -BX、-FX、-FX-FE、または -LX）SFP モジュールのデフォルトは **full** です。二重オプションは、1000BASE-x（-x は -BX、-CWDM、-LX、-SX、または -ZX）SFP モジュールではサポートされていません。

ご使用のスイッチでサポートされている SFP モジュールについては、製品のリリース ノートを参照してください。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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せん。ただし、これらのインターフェイスを半二重モードで動作するように設定することはできません。

特定のポートを全二重または半二重のいずれかに設定できます。このコマンドの適用可能性は、スイッチが接続されているデバイスによって異なります。

両方のラインの終端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエーションをサポートし、もう片方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定し、サポートされている側で **auto** の設定を使用してください。

速度が **auto** に設定されている場合、スイッチはリンクの反対側のデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。

**注意**

インターフェイス速度およびデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

**例**

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1/1
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   |
|---------------------------------|--|
| <a href="#">show interfaces</a> | スイッチのインターフェイスの設定を表示します。                        |
| <a href="#">speed</a>           | 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 error-disable 検出をイネーブルにするには、グローバル コンフィギュレーション モードで **errdisable detect cause** 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には、このコマンドの **no** 形式を使用します。

```
errdisable detect cause {all | arp-inspection | bpduguard | dhcp-rate-limit | dtp-flap |
gbic-invalid | inline-power | link-flap | loopback | pagp-flap | psp | security-violation
shutdown vlan | sfp-config-mismatch}
```

```
no errdisable detect cause {all | arp-inspection | bpduguard | dhcp-rate-limit | dtp-flap |
gbic-invalid | inline-power | link-flap | loopback | pagp-flap | psp | security-violation
shutdown vlan | sfp-config-mismatch}
```

```
errdisable detect cause bpduguard shutdown vlan
```

```
no errdisable detect cause bpduguard shutdown vlan
```

## 構文の説明

|                                |   |
|--------------------------------|---|
| <b>all</b>                     | 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。  |
| <b>arp-inspection</b>          | ダイナミック アドレス解決プロトコル (ARP) インスペクションのエラー検出をイネーブルにします。  |
| <b>bpduguard shutdown vlan</b> | BPDU ガードで VLAN ごとに error-disable を指定します。  |
| <b>dhcp-rate-limit</b>         | DHCP スヌーピングのエラー検出をイネーブルにします。  |
| <b>dtp-flap</b>                | ダイナミック トランッキング プロトコル (DTP) フラップのエラー検出をイネーブルにします。  |
| <b>gbic-invalid</b>            | 無効なギガビット インターフェイス コンバータ (GBIC) モジュール用のエラー検出をイネーブルにします。<br><br>(注) このエラーは、スイッチでの無効な Small Form-Factor Pluggable (SFP) モジュールを意味します。 |
| <b>inline-power</b>            | インライン パワーに対し、エラー検出をイネーブルにします。   |
| <b>link-flap</b>               | 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。   |
| <b>loopback</b>                | 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。  |
| <b>pagp-flap</b>               | ポート集約プロトコル (PAgP) フラップの errdisable 原因のエラー検出をイネーブルにします。  |
| <b>psp</b>                     | プロトコル ストーム プロテクションのエラー検出をイネーブルにします。   |
| <b>security-violation</b>      | 音声認識 802.1x セキュリティをイネーブルにします。   |
| <b>shutdown vlan</b>           |   |
| <b>sfp-config-mismatch</b>     | SFP 設定の不一致によるエラー検出をイネーブルにします。   |

## コマンドデフォルト

検出はすべての原因に対してイネーブルです。VLAN ごとの errdisable を除くすべての原因について、ポート全体をシャットダウンするように設定されます。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

ブリッジプロトコルデータユニット (BPDU) ガードとポートセキュリティについては、このコマンドを使用して、ポート全体をディセーブルにするのではなく、ポートの特定の VLAN のみをディセーブルにするようにスイッチを設定できます。

VLAN ごとに **errdisable** 機能をオフにしている BPDU ガード違反が発生した場合は、ポート全体がディセーブルになります。VLAN ごとに **errdisable** 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

原因 (**link-flap**、**dhcp-rate-limit** など) は、**errdisable** ステートが発生した理由です。原因がポートで検出された場合、ポートは **errdisable** ステート (リンクダウン ステートに類似した動作ステート) となります。

ポートが **errdisable** になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU、音声認識 802.1x セキュリティ、ガードおよびポートセキュリティ機能のため、違反の発生時に、ポート全体でなく、ポート上の障害のある VLAN だけをシャットダウンするようスイッチを設定することができます。

原因に対して **errdisable recovery** グローバル コンフィギュレーション コマンドを入力して、原因の回復メカニズムを設定する場合は、すべての原因がタイムアウトになった時点で、ポートは **errdisable** ステートから抜け出して、処理を再試行できるようになります。回復メカニズムを設定しない場合は、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、ポートを手動で **errdisable** ステートから回復させる必要があります。

プロトコル ストーム プロテクションでは、最大 2 個の仮想ポートについて過剰なパケットがドロップされます。**psp** キーワードを使用した仮想ポート エラーのディセーブル化は、EtherChannel インターフェイスおよび Flexlink インターフェイスでサポートされません。

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。

## 例

次の例では、リンクフラップ **errdisable** 原因の **errdisable** 検出をイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause link-flap
```

次のコマンドでは、VLAN ごとの **errdisable** で BPDU ガードをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
```

次のコマンドでは、VLAN ごとの **errdisable** で音声認識 802.1x セキュリティをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

**show errdisable detect** 特権 EXEC コマンドを入力すると、設定を確認できます。

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">show errdisable detect</a>              | errdisable 検出情報を表示します。   |
| <a href="#">show interfaces status err-disabled</a> | 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。                          |
| <a href="#">clear errdisable interface</a>          | VLAN ごとの errdisable 機能によって errdisable になったポートまたは VLAN から errdisable ステートをクリアします。 |

# errdisable detect cause small-frame

着信 VLAN タグ付きパケットのフレームが小さく (67 バイト以下)、設定された最低速度 (しきい値) で到着する場合に、任意のスイッチ ポートを `errdisable` にすることを許可するには、グローバル コンフィギュレーション モードで `errdisable detect cause small-frame` コマンドを使用します。デフォルト設定に戻すには、このコマンドの `no` 形式を使用します。

`errdisable detect cause small-frame`

`no errdisable detect cause small-frame`

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

この機能はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、小さいフレームの着信機能をグローバルにイネーブルにします。各ポートのしきい値を設定するには、`small violation-rate` インターフェイス コンフィギュレーション コマンドを使用します。

ポートが自動的に再びイネーブルになるように設定するには、`errdisable recovery cause small-frame` グローバル コンフィギュレーション コマンドを使用します。回復時間を設定するには、`errdisable recovery interval interval` グローバル コンフィギュレーション コマンドを使用します。

## 例

次の例では、小さい着信フレームが設定されたしきい値で到着すると `errdisable` モードになるスイッチ ポートをイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause small-frame
```

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

## ■ errdisable detect cause small-frame

| 関連コマンド | コマンド  | 説明  |
|--------|---|---|
|        | <a href="#">errdisable recovery cause small-frame</a> | 回復タイマーをイネーブルにします。                                   |
|        | <a href="#">errdisable recovery</a>                   | 指定された errdisable ステートから回復する時間を指定します。                |
|        | <a href="#">show interfaces</a>                       | 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。                   |
|        | <a href="#">small-frame violation rate</a>            | ポートが errdisable ステートとなる、小さい着信フレームの伝送速度（しきい値）を設定します。 |

# errdisable recovery cause small-frame

スイッチに小さいフレームが着信してポートが **errdisable** になった後でポートを自動的に再有効化する回復タイマーをイネーブルにするには、グローバル コンフィギュレーション モードで **errdisable recovery cause small-frame** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**errdisable recovery cause small-frame**

**no errdisable recovery cause small-frame**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

この機能はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、**errdisable** ポートの回復タイマーをイネーブルにします。回復時間を設定するには、**errdisable recovery interval interval** インターフェイス コンフィギュレーション コマンドを使用します。

## 例

次の例では、回復タイマーを設定する方法を示します。

```
Switch(config)# errdisable recovery cause small-frame
```

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

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">errdisable detect cause small-frame</a> | 着信フレームが指定した最小サイズより小さく、指定した伝送速度（しきい値）で到着する場合に、スイッチ ポートを <b>errdisable</b> 状態にします。 |
| <a href="#">show interfaces</a>                     | 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。  |
| <a href="#">small-frame violation rate</a>          | ポートが <b>errdisable</b> ステートとなる、(小さい) 着信フレームのサイズを設定します。                           |

# errdisable recovery

回復メカニズム変数を設定するには、グローバル コンフィギュレーション モードで **errdisable recovery** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | link-flap | loopback | pagp-flap |
psecure-violation | psp | security-violation | sfp-config-mismatch | udld | vmps} | {interval
interval}}
```

```
no errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | link-flap | loopback | pagp-flap |
psecure-violation | psp | security-violation | sfp-config-mismatch | udld | vmps} | {interval
interval}}
```

## 構文の説明

|                           |   |
|---------------------------|---|
| <b>cause</b>              | 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。  |
| <b>all</b>                | 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。  |
| <b>bpduguard</b>          | ブリッジ プロトコル データ ユニット (BPDU) 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。   |
| <b>channel-misconfig</b>  | EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。  |
| <b>dhcp-rate-limit</b>    | 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。  |
| <b>dtp-flap</b>           | ダイナミック トランッキング プロトコル (DTP) 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。  |
| <b>gbic-invalid</b>       | ギガビット インターフェイス コンバータ (GBIC) モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。<br><b>(注)</b> このエラーは無効な Small Form-Factor Pluggable (SFP) の errdisable ステートを意味します。 |
| <b>inline-power</b>       | インライン パワーに対し、エラー検出をイネーブルにします。   |
| <b>link-flap</b>          | 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。  |
| <b>loopback</b>           | 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。   |
| <b>pagp-flap</b>          | ポート集約プロトコル (PAgP) フラップ errdisable ステートから回復するタイマーをイネーブルにします。   |
| <b>psecure-violation</b>  | 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。   |
| <b>psp</b>                | プロトコル ストーム プロテクションの 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。  |
| <b>security-violation</b> | 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。  |
| <b>udld</b>               | 単方向リンク検出 (UDLD) 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。  |

|                          |   |
|--------------------------|---|
| <b>vmps</b>              | VLAN メンバーシップ ポリシー サーバ (VMPS) 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。   |
| <b>interval interval</b> | 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。<br><br>(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。 |

**コマンド デフォルト**

すべての原因に対して回復はディセーブルです。  
デフォルトの回復間隔は 300 秒です。

**コマンド モード**

グローバル コンフィギュレーション

**コマンド履歴**

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン**

原因 (**link-flap**、**bpduguard** など) は、errdisable ステートが発生した理由として定義されます。原因がポートで検出された場合、ポートは errdisable ステート (リンクダウン ステートに類似した動作ステート) となります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

その原因に対して errdisable の回復をイネーブルにしない場合、ポートは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで errdisable ステートのままです。原因の回復をイネーブルにした場合、ポートは errdisable ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

原因の回復をイネーブルにしない場合、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、手動でポートを errdisable ステートから回復させる必要があります。

**例**

次の例では、BPDU ガード errdisable 原因に対して回復タイマーをイネーブルにする方法を示します。

```
Switch(config)# errdisable recovery cause bpduguard
```

次の例では、タイマーを 500 秒に設定する方法を示します。

```
Switch(config)# errdisable recovery interval 500
```

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

## 関連コマンド

| コマンド   | 説明   |
|--|--|
| <code>clear errdisable interface</code>          | VLAN ごとの errdisable 機能によって errdisable になったポートまたは VLAN から errdisable ステートをクリアします。 |
| <code>show errdisable recovery</code>            | errdisable 回復タイマーの情報を表示します。  |
| <code>show interfaces status err-disabled</code> | 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。                          |

# exception crashinfo

Cisco IOS イメージでエラーが発生した場合は、スイッチが拡張 crashinfo ファイルを作成するように設定するには、グローバル コンフィギュレーション モードで **exception crashinfo** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**exception crashinfo**

**no exception crashinfo**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

スイッチが拡張 crashinfo ファイルを作成します。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

基本 crashinfo ファイルには、失敗した Cisco IOS のイメージ名とバージョン、およびプロセッサ レジスタのリストが含まれます。拡張 crashinfo ファイルには、スイッチの障害の原因を判別するのに役立つその他の追加情報が含まれます。

スイッチが拡張 crashinfo ファイルを作成しないように設定するには、**no exception crashinfo** グローバル コンフィギュレーション コマンドを使用します。

## 例

次の例では、スイッチが拡張 crashinfo ファイルを作成しないように設定する方法を示します。

```
Switch(config)# no exception crashinfo
```

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

## 関連コマンド

| コマンド                       | 説明   |
|----------------------------|--|
| <b>show running-config</b> | 定義されたマクロを含む動作設定を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# fallback profile

Web 認証用にフォールバック プロファイルを作成するには、グローバル コンフィギュレーション モードで **fallback profile** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**fallback profile** *profile*

**no fallback profile**

## 構文の説明

|                |  |
|----------------|--|
| <i>profile</i> | IEEE 802.1x 認証をサポートしていないクライアントのフォールバック プロファイルを指定します。 |
|----------------|--|

## コマンドデフォルト

フォールバック プロファイルは設定されていません。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

フォールバック プロファイルは、サブリカントを持たない IEEE 802.1x ポートの IEEE 802.1x フォールバック動作を定義するために使用されます。サポートされる動作は、Web 認証へのフォールバックだけです。

**fallback profile** コマンドを入力すると、プロファイル コンフィギュレーション モードが開始され、次のコンフィギュレーション コマンドが使用可能になります。

- **ip** : IP コンフィギュレーションを作成します。
- **access-group** : まだ認証されていないホストによって送信されるパケットのアクセス コントロールを指定します。
- **admission** : IP アドミッション ルールを適用します。

## 例

次の例では、Web 認証で使用されるフォールバック プロファイルの作成方法を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

**show running-configuration [interface interface-id]** 特権 EXEC コマンドを入力することにより、設定を確認できます。

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">dot1x fallback</a>                      | 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。 |
| <a href="#">ip admission</a>                        | スイッチ ポートで Web 認証をイネーブルにします。  |
| <a href="#">ip admission name proxy http</a>        | スイッチで Web 認証をグローバルにイネーブルにします。                                      |
| <a href="#">show dot1x [interface interface-id]</a> | 指定されたポートの IEEE 802.1x の状態を表示します。                                   |
| <a href="#">show fallback profile</a>               | スイッチの設定済みプロファイルを表示します。   |

# fcs-threshold

フレーム チェック シーケンス (FCS) のビット エラー レートを設定するには、インターフェイス コンフィギュレーション モードで **fcs-threshold** 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。

## コマンドデフォルト

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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。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 レートに接近すると切り替わる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  |
|--------------------------------------|---|
| <b>alarm facility fcs-hysteresis</b> | 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。 |
| <b>show fcs-threshold</b>            | 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。              |

# fixup

一部のプロトコルは、レイヤ 2 で NAT 間で透過的に動作しません。これらのプロトコルは、Application Layer Gateway (ALG) を使用して「修正」する必要があります。ARP と ICMP の修正はデフォルトでイネーブルです。レイヤ 2 NAT インスタンスに対するこれらの設定を変更するには、config l2nat モードで **fixup** コマンドを使用します。

指定したプロトコルのフィックスアップをディセーブルにするには、このコマンドの **no** 形式を入力します。

```
fixup { arp | icmp | all }
no fixup { arp | icmp | all }
```

## 構文の説明

|             |                       |
|-------------|-----------------------|
| <b>arp</b>  | ARP を修正します            |
| <b>icmp</b> | ICMP を修正します           |
| <b>all</b>  | ARP と ICMP を両方とも修正します |

## コマンドデフォルト

イネーブル

## コマンドモード

Config-l2nat

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(2)EB | このコマンドが導入されました。 |

## 使用上のガイドライン

各レイヤ 2 NAT インスタンスに対するこれらの設定を行います。

## 例

次に、レイヤ 2 NAT インスタンスの ARP をイネーブルにする例を示します。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# fixup arp
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                           |
| <a href="#">show l2nat interface</a>            | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。                |
| <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# 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、インターフェイス コンフィギュレーション モードで、**flowcontrol** コマンドを使用します。

**flowcontrol receive {desired | off | on}**

## 構文の説明

|                |   |
|----------------|---|
| <b>receive</b> | インターフェイスがリモート デバイス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。  |
| <b>desired</b> | 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。 |
| <b>off</b>     | 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。  |
| <b>on</b>      | 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。 |

## コマンドデフォルト

デフォルトは、**flowcontrol receive off** に設定されています。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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。



(注)

スイッチは、ポーズ フレームを受信できますが、送信はできません。

このスイッチでは、送信フロー制御の休止フレームはサポートされません。

**on** および **desired** キーワードは同一の結果になることに注意してください。

**flowcontrol** コマンドを使用してポートが輻輳中にトラフィック レートを制御するよう設定する場合、フロー制御はポート上で次の条件のうちの 1 つに設定されます。

- **receive on** または **desired** : ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要がある装置、または送信可能な接続装置と連動できます。ポートはポーズ フレームを受信できます。
- **receive off** : フロー制御はどちらの方向にも動作しません。輻輳が生じて、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 2-6 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 2-6 フロー制御設定およびローカル/リモート ポート フロー制御解決

| フロー制御設定              |                          | フロー制御解決    |            |
|----------------------|--------------------------|------------|------------|
| ローカル デバイス            | リモート デバイス                | ローカル デバイス  | リモート デバイス  |
| send off/receive on  | send on/receive on       | 受信だけ行います。  | 送受信を行います。  |
|                      | send on/receive off      | 受信だけ行います。  | 送信だけ行います。  |
|                      | send desired/receive on  | 受信だけ行います。  | 送受信を行います。  |
|                      | send desired/receive off | 受信だけ行います。  | 送信だけ行います。  |
|                      | send off/receive on      | 受信だけ行います。  | 受信だけ行います。  |
|                      | send off/receive off     | 送受信を行いません。 | 送受信を行いません。 |
| send off/receive off | send on/receive on       | 送受信を行いません。 | 送受信を行いません。 |
|                      | send on/receive off      | 送受信を行いません。 | 送受信を行いません。 |
|                      | send desired/receive on  | 送受信を行いません。 | 送受信を行いません。 |
|                      | send desired/receive off | 送受信を行いません。 | 送受信を行いません。 |
|                      | send off/receive on      | 送受信を行いません。 | 送受信を行いません。 |
|                      | send off/receive off     | 送受信を行いません。 | 送受信を行いません。 |

**例** 次の例では、リモート ポートによってフロー制御がサポートされないようにローカル ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet 1/1
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                                |
|---------------------------------|-----------------------------------|
| <a href="#">show interfaces</a> | 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。 |

# inside from

外部アドレスに内部アドレスを変換するには、`config-l2nat` モードで **inside from** コマンドを入力します。変換を削除するには、このコマンドの **no** 形式を使用します。

```
inside from {host | range | network} original ip to translated ip [mask] number | mask
```

```
no inside from {host | range | network} original ip to translated ip [mask] number | mask
```

## 構文の説明

|                                     |   |
|-------------------------------------|---|
| <b>host</b>                         | 単一のホストアドレスを変換します。   |
| <b>range</b>                        | ホストアドレス範囲を変換します。 <i>number</i> を入力して範囲のサイズを指定します。   |
| <b>network</b>                      | サブネット内のすべてのホストアドレスを変換します。ホストのオクテットは 1.1.0.0 のように 0 にする必要があります。別の値を入力した場合、無視されます。 <i>translated ip</i> を入力する場合、 <b>mask mask</b> を含めます。                  |
| <i>original ip to translated ip</i> | ホストのプライベート IP アドレス、範囲、またはネットワークおよび対応するパブリック IP アドレス。  |
| <b>mask mask</b>                    | <b>network</b> オプションを使用する場合以外は任意です。サブネットマスク。有効なサブネットは 255.255.0.0、255.255.255.0、255.255.255.128、255.255.255.192、255.255.255.224、および 255.255.255.240 です。 |
| <i>number</i>                       | <b>range</b> オプションを使用する場合以外は任意です。範囲のサイズ。  |

## コマンド デフォルト

なし

## コマンド モード

Config-l2nat モード

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(2)EB | このコマンドが導入されました。 |

## 使用上のガイドライン

- 各レイヤ 2 NAT インスタンスの変換を設定します。
- 指定されたレイヤ 2 NAT インスタンスがすでにある場合、新しい変換値は前述のリストに追加されます。
- 内部ネットワークのデバイスから外部ネットワーク デバイスに **ping** を実行するには、外部デバイスの変換済みアドレスを使用します。たとえば、外部ホスト 10.10.10.100 が内部ホスト 192.168.1.100 に変換される場合は、**ping 192.168.1.100** です。
- 範囲：
  - 範囲は互いに重複させないでください。
  - 範囲は /24 のネットワーク設定と重複させないでください。
  - オリジナルと変換された IP アドレスは 1 対 1 に対応させる必要があります (x.x.x.1 ~ y.y.y.1、x.x.x.2 ~ x.x.x.2 など)。元のアドレスおよび変換されたアドレスがこのように対応していない場合は、**host** コマンドを使用して各アドレスを個別に設定できます。
- 各変換の個別の統計情報は **host** および **range** オプションを使用して変換されるアドレスには利用できますが、**network** オプションによって変換されるアドレスには利用できません。

## 例

次に、内部アドレス 192.168.0.100 を外部アドレス 10.1.0.100 に変換するように、Instance1 という名前のインスタンスを設定する例を示します。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# inside from host 192.168.0.100 to 10.1.0.100
```

次に、5つの内部アドレスの範囲を対応する外部アドレスに変換するように、Instance1 という名前のインスタンスを設定する例を示します。192.168.142.1 は 10.10.10.1、192.168.142.2 は 10.10.10.2 などに変換されます。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# inside from range 192.168.142.1 to 10.10.10.1 5
```

次に、内部サブネット上のすべてのアドレスを外部サブネット上の対応するアドレスに変換するように、Instance1 という名前のインスタンスを設定する例を示します。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# inside from network 192.168.142.0 to 20.20.30.0 mask 255.255.255.0
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">outside from</a>                    | レイヤ 2 NAT を使用して、外部アドレスを内部アドレスに変換します。                        |
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                           |
| <a href="#">show l2nat interface</a>            | 1つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。                 |
| <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# interface port-channel

ポート チャネル論理インターフェイスのアクセスまたは作成を行うには、グローバル コンフィギュレーション モードで **interface port-channel** 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。範囲は 1 ~ 6 です。

## コマンドデフォルト

ポート チャネル論理インターフェイスは定義されません。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

レイヤ 2 EtherChannel では、物理ポートをチャネル グループに割り当てる前にポートチャネル インターフェイスを作成する必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。チャネル グループが最初の物理ポートを獲得すると、ポートチャネル インターフェイスは自動的に作成されます。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

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

チャネル グループ内の 1 つのポート チャネルだけが許可されます。



### 注意

ポート チャネル インターフェイスをルーテッド ポートとして使用する場合、チャネル グループに割り当てられた物理ポート上のレイヤ 3 に、アドレスを割り当てないようにしてください。



### 注意

レイヤ 3 のポート チャネル インターフェイスとして使用されているチャネル グループの物理ポート上で、ブリッジ グループを割り当てることは、ループ発生の原因になるため行わないようにしてください。スパニングツリーもディセーブルにする必要があります。

**interface port-channel** コマンドを使用する場合は、次の注意事項に従ってください。

- Cisco Discovery Protocol (CDP) を使用する場合には、これを物理ポートでだけ設定してください。ポート チャンネル インターフェイスでは設定できません。
- EtherChannel のアクティブ メンバであるポートを IEEE 802.1x ポートとしては設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、そのポートは EtherChannel に加入しません。

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

## 例

次の例では、ポート チャンネル番号 5 でポートチャンネル 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  |
|----------------------------|---|
| <b>channel-group</b>       | EtherChannel グループにイーサネット ポートを割り当てます。  |
| <b>show etherchannel</b>   | チャンネルの EtherChannel 情報を表示します。   |
| <b>show running-config</b> | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# interface range

インターフェイスの範囲を入力し、複数のポートでコマンドを同時に実行するには、グローバル コンフィギュレーション モードで **interface range** 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 {type | id} {port-range | macro name}
```

```
no interface range {port-range | macro name}
```

## 構文の説明

|                   |  |
|-------------------|--|
| <i>port-range</i> | ポート範囲。 <i>port-range</i> の有効値のリストについては、「Usage Guidelines (使用上のガイドライン)」を参照してください。 |
| <i>macro name</i> | マクロ名を指定します。  |

## コマンド デフォルト

なし

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 スイッチ仮想インターフェイス (SVI) 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。

- fastethernet module/{first port} - {last port}**,
  - 使用可能範囲は、*type number/number - number* です (例 : **gigabitethernet1/1 - 2**)。
- loopback loopback-number - loopback number : loopback-number** は 1 ~ 2147483647
- port-channel port-channel-number - port-channel-number : port-channel-number** は 1 ~ 6 です



(注) ポートチャネルの **interface range** コマンドを使用した場合、範囲内の最初と最後のポートチャネル番号はアクティブなポートチャネルである必要があります。

- **tunnel tunnel-number - tunnel-number** : tunnel-number は 1 ~ 2147483647
- **vlan vlan-ID - vlan-ID** (vlan ID の範囲は 1 ~ 4094)

範囲を定義するときは、最初の入力とハイフン (-) の間にスペースが必要です。

```
interface range gigabitethernet1/1 -2
```

範囲を複数定義するときでも、最初のエントリとカンマ (,) の間にスペースを入れる必要があります。

```
interface range fastethernet1/1 - 2, gigabitethernet1/1 - 2
```

同じコマンドでマクロとインターフェイス範囲の両方を指定することはできません。

また、*port-range* で単一インターフェイスを指定することもできます。つまりこのコマンドは、**interface interface-id** グローバル コンフィギュレーション コマンドに類似しています。

インターフェイスの範囲の設定に関する詳細は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

## 例

次の例では、**interface range** コマンドを使用して、インターフェイス範囲コンフィギュレーションモードを開始し、2つのポートにコマンドを入力する方法を示します。

```
Switch(config)# interface range gigabitethernet1/1 - 2
```

次の例では、同じ機能に対して1つのポート範囲マクロ **macrol** を使用する方法を示します。この利点は、**macrol** を削除するまで再利用できることです。

```
Switch(config)# define interface-range macrol gigabitethernet1/1 - 2
Switch(config)# interface range macro macrol
Switch(config-if-range)#
```

## 関連コマンド

| コマンド                                   | 説明  |
|--|---|
| <a href="#">define interface-range</a> | インターフェイス範囲のマクロを作成します。   |
| <a href="#">show running-config</a>    | スイッチで現在の動作設定情報を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# ip access-group

レイヤ 2 またはレイヤ 3 interface へのアクセスを制御するには、インターフェイス コンフィギュレーション モードで **ip access-group** コマンドを使用します。インターフェイスからすべてまたは指定のアクセス グループを削除するには、このコマンドの **no** 形式を使用します。

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

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

## 構文の説明

|                           |   |
|---------------------------|---|
| <i>access-list-number</i> | IP アクセス コントロール リスト (ACL) 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>               | <b>ip access-list</b> 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。      |
| <b>in</b>                 | 入力パケットに対するフィルタリングを指定します。  |
| <b>out</b>                | 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。           |

## コマンド デフォルト

アクセス リストは、インターフェイスには適用されません。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

名前付きまたは番号付きの標準/拡張 IP アクセス リストをインターフェイスに適用できます。名前を付けてアクセス リストを定義するには、**ip access-list** グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストを定義するには、**access list** グローバル コンフィギュレーション コマンドを使用します。1 ~ 99 および 1300 ~ 1999 の範囲の番号付き標準アクセス リスト、または 100 ~ 199 および 2000 ~ 2699 の範囲の番号付き拡張アクセス リストを使用できます。

このコマンドを使用して、アクセス リストをレイヤ 2 またはレイヤ 3 のインターフェイスに適用できます。ただし、レイヤ 2 のインターフェイス (ポート ACL) には、次のような制限があることに注意してください。

- ACL は受信方向のレイヤ 2 ポートにだけ適用できます。
- インターフェイスごとに 1 つの IP ACL と 1 つの MAC ACL だけを適用できます。
- レイヤ 2 のインターフェイスはログギングをサポートしていません。**log** キーワードが IP ACL で指定された場合、無視されます。
- レイヤ 2 のインターフェイスに適用された IP ACL は、IP パケットだけをフィルタにかけます。非 IP パケットをフィルタリングするには、MAC 拡張 ACL とともに **mac access-group** インターフェイス コンフィギュレーション コマンドを使用します。



(注)

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 はルータ ACL または VLAN マップよりも優先されます。ルータの ACL は IP サービスイメージが実行されているスイッチでのみサポートされます。

- 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と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）、インターネット制御メッセージプロトコル（ICMP）の Host Unreachable のメッセージが生成されます。ICMP Host Unreachable メッセージは、レイヤ 2 インターフェイスでドロップされたパケットに対しては生成されません。

通常の発信アクセスリストでは、パケットを受信して、それを制御されたインターフェイスへ送信した後、スイッチがアクセスリストと照合することでパケットを確認します。アクセスリストがパケットを許可した場合、スイッチはパケットを送信します。アクセスリストがパケットを拒否した場合、スイッチはパケットをドロップし、デフォルトの設定では、ICMP Host Unreachable メッセージが生成されます。指定したアクセスリストが存在しない場合は、すべてのパケットが通過します。

**例** 次の例では、ポートの入力パケットに IP アクセスリスト 101 を適用する方法を示します。

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# ip access-group 101 in
```

## 関連コマンド

| コマンド                        | 説明  |
|-----------------------------|---|
| <b>access list</b>          | 番号付き ACL を設定します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。               |
| <b>ip access-list</b>       | 名前付き ACL を設定します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。               |
| <b>show access-lists</b>    | スイッチで設定された ACL を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。         |
| <b>show ip access-lists</b> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。      |
| <b>show ip interface</b>    | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# ip address

レイヤ 2 スイッチの IP アドレスや、各スイッチ仮想インターフェイス (SVI) の IP アドレスまたはレイヤ 3 スイッチのルーテッドポートを設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。IP アドレスを削除したり、IP 処理をディセーブルにしたりするには、このコマンドの **no** 形式を使用します。

**ip address ip-address subnet-mask [secondary]**

**no ip address [ip-address subnet-mask] [secondary]**

## 構文の説明

|                    |  |
|--------------------|--|
| <i>ip-address</i>  | [IP Address]。  |
| <i>subnet-mask</i> | 関連する IP サブネットのマスク。   |
| <b>secondary</b>   | (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。 |

## コマンド デフォルト

IP アドレスは定義されていません。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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、インターネット制御メッセージプロトコル (ICMP) Mask Request メッセージを使用して、サブネット マスクを判別できます。ルータは、この要求に対して ICMP Mask Reply メッセージで応答します。

**no ip address** コマンドを使って IP アドレスを削除することで、特定のインターフェイス上の IP プロセスをディセーブルにできます。スイッチが、その IP アドレスのうちの 1 つを使用している他のホストを検出した場合、コンソールにエラー メッセージを送信します。

オプションで **secondary** キーワードを使用することで、セカンダリ アドレスの番号を無制限に指定することができます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成しないというのを除けば、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。ソフトウェアに、設定できるルーテッドポートおよびSVIの個数制限はありません。この個数と設定されている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スイッチのIPアドレスを設定する方法を示します。

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

次の例では、レイヤ3スイッチ上のポートにIPアドレスを設定する方法を示します。

```
Switch(config)# ip multicast-routing
Switch(config)# interface gigabitethernet1/1
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   |
|----------------------------|--|
| <b>show running-config</b> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# ip admission

Web 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。このコマンドは、**fallback-profile** モードでも使用できます。Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

**ip admission rule**

**no ip admission**

## 構文の説明

|             |                                |
|-------------|--------------------------------|
| <i>rule</i> | IP アドミッション ルールをインターフェイスに適用します。 |
|-------------|--------------------------------|

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**ip admission** コマンドにより、スイッチ ポートに Web 認証ルールが適用されます。

## 例

次の例では、スイッチ ポートに Web 認証ルールを適用する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# ip admission rule1
```

次の例では、IEEE 802.1x 対応のスイッチ ポートで使用するフォールバック プロファイルに Web 認証ルールを適用する方法を示します。

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config)# ip admission name rule1
Switch(config)# end
```

## 関連コマンド

| コマンド   | 説明  |
|--|---|
| <a href="#">dot1x fallback</a>               | 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。  |
| <a href="#">fallback profile</a>             | ポートで Web 認証をイネーブルにします。  |
| <a href="#">ip admission name proxy http</a> | スイッチで Web 認証をグローバルにイネーブルにします。   |
| <a href="#">show ip admission</a>            | NAC のキャッシュされたエントリまたは NAC 設定についての情報を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# ip admission name proxy http

Web 認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ip admission name proxy http** コマンドを使用します。Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

**ip admission name proxy http**

**no ip admission name proxy http**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

Web 認証はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**ip admission name proxy http** コマンドにより、Web 認証がスイッチ上でグローバルにイネーブルになります。

スイッチで Web 認証をグローバルにイネーブルにしてから、**ip access-group in** および **ip admission web-rule** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイスで Web 認証をイネーブルにします。

## 例

次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

次の例では、スイッチ ポートでのフォールバック メカニズムとして、Web 認証とともに IEEE 802.1x 認証を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

## 関連コマンド

| コマンド                              | 説明   |
|-----------------------------------|--|
| <a href="#">dot1x fallback</a>    | 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。   |
| <a href="#">fallback profile</a>  | Web 認証のフォールバック プロファイルを作成します。   |
| <a href="#">ip admission</a>      | ポートで Web 認証をイネーブルにします。   |
| <a href="#">show ip admission</a> | NAC のキャッシュされたエントリまたは NAC 設定についての情報を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# ip arp inspection filter vlan

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、グローバル コンフィギュレーション モードで **ip arp inspection filter vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**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 アクセス コントロール リスト (ACL) の名前  |
| <i>vlan-range</i>   | VLAN の番号または範囲。<br><br>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。  |
| <b>static</b>       | (任意) ARP ACL の暗黙的な拒否を明示的な拒否として処理し、ACL 内の以前の句と一致しないパケットを廃棄します。DHCP バインディングは使用されません。<br><br>このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないこととなります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。 |

## コマンド デフォルト

VLAN には、定義された ARP ACL が適用されていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

ARP ACL がダイナミック ARP インスペクションの VLAN に適用されている場合、IP-to-MAC 15.0(1)EY のアドレス バインディングを持つ 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 インスペクション用に 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  |
|---|---|
| <b>arp access-list</b>                  | ARP ACL を定義します。                                     |
| <b>deny (ARP アクセスリスト コンフィギュレーション)</b>   | 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。               |
| <b>permit (ARP アクセスリスト コンフィギュレーション)</b> | 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。               |
| <b>show arp access-list</b>             | ARP アクセス リストに関する詳細を表示します。                           |
| <b>show inventory vlan vlan-range</b>   | 指定された VLAN のダイナミック ARP インスペクションの設定および動作ステータスを表示します。 |

# ip arp inspection limit

インターフェイスのアドレス解決プロトコル (ARP) の入力要求および応答のレートを制限するには、インターフェイス コンフィギュレーション モードで **ip arp inspection limit** 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 インспекションによってスイッチ 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

|                               |   |
|-------------------------------|---|
| <b>rate pps</b>               | 1 秒間に処理される入力パケット数の上限を指定します。範囲は、0 ~ 2048 pps です。                       |
| <b>burst interval seconds</b> | (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連続的インターバルを秒単位で指定します。範囲は 1 ~ 15 秒です。 |
| <b>none</b>                   | 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。                                       |

## コマンド 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、レート制限は行われません。

バースト インターバルは 1 秒です。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 インспекション対応 VLAN でパケットを処理するようにトランクに適切なレートを設定するか、**none** キーワードを使用してレートを無制限にします。

スイッチが、設定されているレートを超えるレートのパケットを、バーストの秒数を超える連続する秒数受信すると、インターフェイスが **errdisable** ステートになります。

インターフェイス上のレート制限を明示的に設定しない限り、インターフェイスの信頼状態を変更することは、レート制限を信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

トランク ポートは、集約が反映されるように、より大きいレートに設定する必要があります。着信パケットのレートが、ユーザが定義したレートを超えると、スイッチはインターフェイスを **errdisable** ステートにします。**errdisable** 回復機能は、回復の設定に従ってポートを **errdisable** ステートから自動的に移行させます。

EtherChannel ポートの着信 ARP パケットのレートは、すべてのチャネル メンバの着信 ARP パケットレートの合計と同じです。EtherChannel ポートのレート制限は、必ずすべてのチャネル メンバの着信 ARP パケットのレートを調べてから設定してください。

## 例

次の例では、ポート上の着信 ARP 要求のレートを 25 pps に制限し、インターフェイスのモニタリングインターバルを 5 秒間に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1  
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   |
|---|--|
| <a href="#">show inventory interfaces</a> | 指定のインターフェイス、またはすべてのインターフェイスに対して、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 アドレス解決プロトコル (ARP) インспекションのロギング バッファを設定するには、グローバル コンフィギュレーション モードで **ip arp inspection log-buffer** コマンドを使用します。デフォルト設定に戻すには、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

|                         |   |
|-------------------------|---|
| <b>entries number</b>   | バッファに記録されるエントリを指定します。指定できる範囲は 0 ~ 1024 です。  |
| <b>logs number</b>      | システム メッセージを生成するために、指定された間隔に必要なエントリを指定します。   |
| <b>interval seconds</b> | 指定できる <b>interval seconds</b> の範囲は 0 ~ 86400 秒 (1 日) です。0 は、システム メッセージがただちに生成されることを意味します。この場合、ログ バッファは常に空となります。 |

## コマンドデフォルト

ダイナミック ARP がイネーブル、拒否またはドロップされると、ARP パケットが記録されます。ログ エントリ数は、32 です。システム メッセージ数は、毎秒 5 つに制限されます。ロギングレート インターバルは、1 秒です。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。このエントリに対しては、その他の統計情報は表示されません。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                                      |
|---------------------------------------|---|
| <b>arp access-list</b>                | ARP アクセスコントロールリスト (ACL) を定義します。         |
| <b>clear ip arp inspection log</b>    | ダイナミック ARP インスペクション ログバッファをクリアします。      |
| <b>ip arp inspection vlan logging</b> | VLAN 単位で記録するパケットのタイプを制御します。             |
| <b>show inventory log</b>             | ダイナミック ARP インスペクション ログバッファの設定と内容を表示します。 |

# ip arp inspection trust

検査対象の着信アドレス解決プロトコル (ARP) パケットを指定するインターフェイスの信頼状態を設定するには、インターフェイス コンフィギュレーション モードで **ip arp inspection trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**ip 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。

## コマンドデフォルト

インターフェイスは、信頼できない状態です。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。

## 例

次の例では、ポートを信頼できる状態に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
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   |
|---|--|
| <code>ip arp inspection log-buffer</code> | ダイナミック ARP インспекション ログ バッファを設定します。                          |
| <code>show inventory interfaces</code>    | 指定のインターフェイス、またはすべてのインターフェイスに対して、ARP パケットの信頼状態およびレート制限を表示します。 |
| <code>show inventory log</code>           | ダイナミック ARP インспекション 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 アドレス解決プロトコル (ARP) インспекションの特定のチェックを実行するには、グローバル コンフィギュレーション モードで **ip arp inspection validate** コマンドを使用します。デフォルト設定に戻すには、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

|                    |  |
|--------------------|--|
| <b>src-mac</b>     | (任意) イーサネット ヘッダーの送信元 MAC アドレスを ARP 本文の送信側 MAC アドレスと比較します。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。<br><br>イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。   |
| <b>dst-mac</b>     | (任意) イーサネット ヘッダーの宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較します。この検査は、ARP 応答に対して実行されます。<br><br>イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。   |
| <b>ip</b>          | (任意) ARP 本文を確認して、無効な IP アドレスや予期しない IP アドレスがないかを比較します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。<br><br>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。 |
| <b>allow-zeros</b> | (任意) 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。  |

## コマンド デフォルト

検査は実行されません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 アクセス コントロール リスト (ACL) と連動します。

- ARP ACL が ARP プローブを拒否するように設定されている場合は、**allow-zero** キーワードが指定されていても、ARP プローブはドロップされます。
- ARP プローブを明確に許可する ARP ACL を設定し、**ip arp inspection validate ip** コマンドを設定する場合、**allow-zeros** キーワードを入力しない限り、ARP プローブはドロップされます。

このコマンドの **no** 形式を使用すると、指定されたチェックだけがディセーブルになります。どのオプションもイネーブルにしない場合は、すべてのチェックがディセーブルになります。

#### 例

次に、送信元 MAC の検証をイネーブルにする例を示します。

```
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   |
|---|--|
| <b>show inventory vlan<br/>vlan-range</b> | 指定された VLAN のダイナミック ARP インспекション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 アドレス解決プロトコル (ARP) インスペクションをイネーブルにするには、グローバル コンフィギュレーション モードで **ip arp inspection vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**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。<br><br>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。 |
|-------------------|---|

## コマンドデフォルト

すべての VLAN で ARP インスペクションはディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

ダイナミック ARP インスペクション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 インスペクションは、アクセス ポート、トランク ポート、または EtherChannel 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 インスペクション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  |
|--|---|
| <a href="#">arp access-list</a>                              | ARP アクセス コントロール リスト (ACL) を定義します。                   |
| <a href="#">show inventory</a> <b>vlan</b> <i>vlan-range</i> | 指定された VLAN のダイナミック ARP インスペクション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 単位で記録するパケットのタイプを制御するには、グローバル コンフィギュレーション モードで **ip arp inspection vlan logging** コマンドを使用します。このロギング制御をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings {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>   | ロギング用に設定された VLAN。<br><br>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。  |
| <b>acl-match</b> { <b>matchlog</b>   <b>none</b> }                | アクセス コントロール リスト (ACL) との一致に基づいたパケットのロギングを指定します。<br><br>キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>matchlog</b> : アクセス コントロール エントリ (ACE) に指定されたロギング設定に基づいてパケットを記録します。このコマンドに <b>matchlog</b> キーワード、<b>permit</b> または <b>deny</b> ARP アクセス リスト コンフィギュレーション コマンドに <b>log</b> 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アドレス解決プロトコル (ARP) パケットが記録されます。</li> <li><b>none</b> : ACL に一致するパケットを記録しません。</li> </ul> |
| <b>dhcp-bindings</b> { <b>permit</b>   <b>all</b>   <b>none</b> } | 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。<br><br>キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>all</b> : DHCP バインディングと一致するすべてのパケットをロギングします。</li> <li><b>none</b> : DHCP バインディングに一致するパケットを記録しません。</li> <li><b>permit</b> : DHCP バインディングで許可されたパケットをロギングします。</li> </ul>  |
| <b>arp-probe</b>  | 具体的に許可されたパケットが ARP プロブである場合に、パケットのロギングを指定します。   |

## コマンド 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 プロブ パケットは記録されません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 インспекション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   |
|---------------------------------------|--|
| <b>arp access-list</b>                | ARP ACL を定義します。                                      |
| <b>clear ip arp inspection log</b>    | ダイナミック ARP インспекション ログ バッファをクリアします。                 |
| <b>ip arp inspection log-buffer</b>   | ダイナミック ARP インспекション ロギング バッファを設定します。                |
| <b>show inventory log</b>             | ダイナミック ARP インспекション ログ バッファの設定と内容を表示します。            |
| <b>show inventory vlan vlan-range</b> | 指定された VLAN のダイナミック ARP インспекションの設定および動作ステータスを表示します。 |

# 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、グローバル コンフィギュレーション モードで **ip dhcp snooping** コマンドを使用します。デフォルト設定に戻すには、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。

## コマンドデフォルト

DHCP スヌーピングは、ディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

DHCP スヌーピング設定を有効にするには、DHCP スヌーピングをグローバルにイネーブルにする必要があります。

**ip dhcp snooping vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用して VLAN 上でスヌーピングをイネーブルにするまで DHCP スヌーピングはアクティブになりません。

## 例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

## 関連コマンド

| コマンド  | 説明                             |
|---|--------------------------------|
| <a href="#">ip dhcp snooping vlan</a>         | VLAN 上で DHCP スヌーピングをイネーブルにします。 |
| <a href="#">show ip igmp snooping</a>         | DHCP スヌーピング設定を表示します。           |
| <a href="#">show ip dhcp snooping binding</a> | 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、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、特権 EXEC モードで **ip dhcp snooping binding** 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

|                               |  |
|-------------------------------|--|
| <b>mac-address</b>            | MAC アドレス。  |
| <b>vlan vlan-id</b>           | VLAN 番号を指定します。指定できる範囲は 1 ~ 4094 です。                                |
| <b>ip-address</b>             | IP アドレス。   |
| <b>interface interface-id</b> | 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。                              |
| <b>expiry seconds</b>         | 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。 |

## コマンド デフォルト

デフォルトのデータベースは定義されていません。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、スイッチをテストまたはデバッグするときに使用します。

DHCP スヌーピング バインディング データベースでは、各データベース エントリ (別名、バインディング) には、IP アドレス、関連付けられた MAC アドレス、リース時間 (16 進数)、バインディングが適用されるインターフェイス、およびインターフェイスが所属する VLAN が含まれます。データベースには、8192 のバインディングを含めることができます。

設定されたバインディングだけを表示するには、**show ip dhcp snooping binding** 特権 EXEC コマンドを使用します。動的および静的に設定されたバインディングを表示するには、**show ip source binding** 特権 EXEC コマンドを使用します。

## 例

次の例では、VLAN 1 のポートに、有効期限が 1000 秒の DHCP バインディング設定を生成する方法を示します。

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet1/1 expiry 1000
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">ip dhcp snooping</a>              | VLAN 上で DHCP スヌーピングをイネーブルにします。                            |
| <a href="#">show ip dhcp snooping binding</a> | 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。 |
| <a href="#">show ip source binding</a>        | 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、グローバル コンフィギュレーション モードで **ip dhcp snooping database** 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 |
rcp://user@host/filename | tftp://host/filename} | timeout seconds | write-delay seconds}

no ip dhcp snooping database [timeout | write-delay]
```

## 構文の説明

|   |   |
|---|---|
| <b>flash:/filename</b>  | 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。  |
| <b>ftp://user:password@host/filename</b>  | 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。   |
| <b>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b> | 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。   |
| <b>rcp://user@host/filename</b>   | データベース エージェントまたはバインディング ファイルがリモート コピー プロトコル (RCP) サーバにあることを指定します。   |
| <b>tftp://host/filename</b>   | 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。  |
| <b>timeout seconds</b>  | データベース転送プロセスを打ち切るまでの時間 (秒) を指定します。<br><br>デフォルトは 300 秒です。指定できる範囲は 0 ~ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。 |
| <b>write-delay seconds</b>  | 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。   |

## コマンド デフォルト

データベース エージェントまたはバインディング ファイルの URL は、定義されていません。  
タイムアウト値は、300 秒 (5 分) です。  
書き込み遅延値は、300 秒 (5 分) です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

DHCP スヌーピング バインディング データベースには、8192 のバインディングを含めることができます。

データベース内のリース時間を正確な時間にするには、ネットワーク タイム プロトコル (NTP) 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書き込む前に、この URL に空のファイルを作成しておく必要があります。

DHCP スヌーピング バインディング データベースを NVRAM に保存するには、**ip dhcp snooping database flash:/filename** コマンドを使用します。**ip dhcp snooping database timeout** コマンドに 0 秒を設定し、データベースを TFTP ファイルに書き込んでいるときに、TFTP サーバがダウンした場合、データベース エージェントは転送を無期限に続けようとします。この転送が進行中の際、他の転送は開始されません。サーバがダウンしている場合、ファイルを書き込むことができないため、これはあまり重要ではありません。

エージェントをディセーブルにするには、**no ip dhcp snooping database** コマンドを使用します。

タイムアウト値をリセットするには、**no ip dhcp snooping database timeout** コマンドを使用します。

書き込み遅延値をリセットするには、**no ip dhcp snooping database write-delay** コマンドを使用します。

## 例

次の例では、IP アドレス 10.1.1.1 の directory という名前のディレクトリ内にバインディング ファイルを保存する方法を示します。TFTP サーバに file という名前のファイルが存在しなければなりません。

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

次の例では、NVRAM に file01.txt というバインディング ファイルを保存する方法を示します。

```
Switch(config)# ip dhcp snooping database flash:file01.txt
```

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

## 関連コマンド

| コマンド                                  | 説明                                     |
|---------------------------------------|--|
| <b>ip dhcp snooping</b>               | VLAN 上で DHCP スヌーピングをイネーブルにします。         |
| <b>ip dhcp snooping binding</b>       | 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。      |
| <b>show ip dhcp snooping database</b> | 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、グローバル コンフィギュレーション モードで **ip dhcp snooping information option** 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。

## コマンドデフォルト

DHCP オプション 82 データは挿入されます。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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じサブネット上にある場合は、サーバはこの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

次に、DHCP Option 82 データ挿入をイネーブルにする例を示します。

```
Switch(config)# ip dhcp snooping information option
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

## 関連コマンド

| コマンド  | 説明                           |
|---|------------------------------|
| <a href="#">show ip dhcp snooping</a>         | DHCP スヌーピング設定を表示します。         |
| <a href="#">show ip dhcp snooping binding</a> | DHCP スヌーピング バインディング情報を表示します。 |

# ip dhcp snooping information option allow-untrusted

オプション 82 情報を持つ DHCP パケットを、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したアグリゲーション スイッチで受信する場合は、グローバル コンフィギュレーション モードで **ip dhcp snooping information option allow-untrusted** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**ip dhcp snooping information option allow-untrusted**

**no ip dhcp snooping information option allow-untrusted**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

スイッチは、エッジ スイッチに接続されている信頼できないポートで受信する、オプション 82 情報を持つ DHCP パケットをドロップします。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 アドレス解決プロトコル (ARP) インスペクションなどの DHCP セキュリティ機能をイネーブルにすることもできます。ただし、アグリゲーション スイッチで DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないポートで受信されたオプション 82 情報を持つパケットをドロップし、信頼できるインターフェイスに接続されたデバイスの DHCP スヌーピング バインディングを学習しません。

ホストに接続されたエッジ スイッチがオプション 82 情報を挿入する場合に、アグリゲーション スイッチで DHCP スヌーピングを使用するには、アグリゲーション スイッチで **ip dhcp snooping information option allow-untrusted** コマンドを入力します。アグリゲーション スイッチは信頼できないポートで DHCP スヌーピング パケットを受信しますが、ホストのバインディングを学習できます。アグリゲーション スイッチで DHCP セキュリティ機能をイネーブルにすることも可能です。アグリゲーション スイッチが接続されているエッジ スイッチ上のポートは、信頼できるポートとして設定する必要があります。



(注)

信頼できないデバイスが接続されたアグリゲーション スイッチに **ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。

**例** 次の例では、アクセススイッチが、エッジスイッチからの信頼できないパケットのオプション 82 情報を確認せずに、パケットを受け入れるように設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option allow-untrusted
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

**関連コマンド**

| コマンド  | 説明                           |
|---|------------------------------|
| <a href="#">show ip dhcp snooping</a>         | DHCP スヌーピング設定を表示します。         |
| <a href="#">show ip dhcp snooping binding</a> | 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、グローバル コンフィギュレーション モードで **ip dhcp snooping information option format remote-id** 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

|                                   |  |
|-----------------------------------|--|
| <b>string</b> <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。 |
| <b>hostname</b>                   | スイッチのホスト名をリモート ID として指定します。                    |

## コマンド デフォルト

スイッチの MAC アドレスは、リモート ID です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                   |
|---------------------------------------|----------------------|
| <a href="#">show ip dhcp snooping</a> | 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秒単位で受信できる DHCP メッセージ数を設定するには、インターフェイス コンフィギュレーション モードで **ip dhcp snooping limit rate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**ip dhcp snooping limit rate rate**

**no ip dhcp snooping limit rate**

## 構文の説明

*rate* インターフェイスが 1 秒あたりに受信することのできる DHCP メッセージの数。指定できる範囲は 1 ~ 2048 です。

## コマンド デフォルト

DHCP スヌーピング レート制限は、ディセーブルです。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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
```

## 関連コマンド

| コマンド  | 説明                           |
|---|------------------------------|
| <a href="#">errdisable recovery</a>           | 回復メカニズムを設定します。               |
| <a href="#">show ip dhcp snooping</a>         | DHCP スヌーピング設定を表示します。         |
| <a href="#">show ip dhcp snooping binding</a> | 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 スヌーピングでは信頼できるポートとしてポートを設定するには、インターフェイス コンフィギュレーション モードで **ip dhcp snooping trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**ip dhcp 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。

## コマンドデフォルト

DHCP スヌーピング信頼は、ディセーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

DHCP サーバ、その他のスイッチ、またはルータに接続されたポートを信頼できるポートとして設定します。DHCP クライアントに接続されたポートを信頼できないポートとして設定します。

## 例

次の例では、ポート上で DHCP スヌーピング信頼をイネーブルにする方法を示します。

```
Switch(config-if)# ip dhcp snooping trust
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

## 関連コマンド

| コマンド  | 説明                           |
|---|------------------------------|
| <a href="#">show ip dhcp snooping</a>         | DHCP スヌーピング設定を表示します。         |
| <a href="#">show ip dhcp snooping binding</a> | 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

DHCP パケットの送信元 MAC アドレスがクライアントのハードウェア アドレスに一致するようにスイッチを信頼できないポート上で確認するように設定するには、グローバル コンフィギュレーション モードで **ip dhcpsnooping verify** 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。

## コマンドデフォルト

スイッチは、パケットのクライアント ハードウェア アドレスと一致する信頼されないポートで受信した DHCP パケットの送信元 MAC アドレスを確認します。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

サービスプロバイダー ネットワークで、スイッチが信頼できないポートの DHCP クライアントからパケットを受信した場合、スイッチは自動的に送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致するかを確認します。アドレスが一致する場合、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

## 例

次の例では、MAC アドレス確認をディセーブルにする方法を示します。

```
Switch(config)# no ip dhcp snooping verify mac-address
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                  | 説明                   |
|---------------------------------------|----------------------|
| <a href="#">show ip dhcp snooping</a> | DHCP スヌーピング設定を表示します。 |

# ip dhcp snooping vlan

VLAN 上で DHCP スヌーピングをイネーブルにするには、グローバル コンフィギュレーション モードで **ip dhcp snooping vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**ip dhcp snooping vlan** *vlan-range*

**no ip dhcp snooping vlan** *vlan-range*

## 構文の説明

|                   |  |
|-------------------|--|
| <i>vlan-range</i> | 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。<br><br>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。 |
|-------------------|--|

## コマンドデフォルト

すべての VLAN 上で DHCP スヌーピングがディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

VLAN 上で DHCP スヌーピングをイネーブルにする前に、まず DHCP スヌーピングをグローバルにイネーブルにする必要があります。

## 例

次の例では、DHCP スヌーピングを VLAN 10 でイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping vlan 10
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

## 関連コマンド

| コマンド  | 説明                           |
|---|------------------------------|
| <a href="#">show ip dhcp snooping</a>         | DHCP スヌーピング設定を表示します。         |
| <a href="#">show ip dhcp snooping binding</a> | 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 サーキット ID サブオプションを設定するには、インターフェイス コンフィギュレーション モードで **ip dhcp snooping vlan information option format-type circuit-id string** コマンドを使用します。デフォルトのサーキット ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

```
ip dhcp snooping vlan vlan-id information option format-type circuit-id [override] string ASCII-string
```

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



(注)

このコマンドは IP サービス イメージが実行されているスイッチでのみサポートされます。

## 構文の説明

|                                   |   |
|-----------------------------------|---|
| <b>vlan</b> <i>vlan-id</i>        | VLAN ID を指定します。指定できる範囲は 1 ~ 4094 です。                |
| <b>override</b>                   | (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。 |
| <b>string</b> <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。   |

## コマンド デフォルト

**vlan-mod-port** 形式のスイッチ VLAN およびポート ID は、デフォルトのサーキット ID です。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

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

## 例

次の例では、オプション 82 サーキット ID サブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
string customerABC-250-0-0
```

次の例では、オプション 82 サーキット ID 上書きサブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
override string testcustomer
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。



## (注)

リモート ID 設定を含むグローバル コマンド出力だけを表示するには、**show ip dhcp snooping** ユーザ EXEC コマンドを使用します。サーキット ID として設定したインターフェイス単位または VLAN 単位の文字列は表示されません。

## 関連コマンド

| コマンド  | 説明                              |
|---|---------------------------------|
| <b>ip dhcp snooping information option format remote-id</b> | オプション 82 リモート ID サブオプションを設定します。 |
| <b>show ip dhcp snooping</b>                                | DHCP スヌーピング設定を表示します。            |

# ip igmp filter

レイヤ 2 インターフェイス上のすべてのホストがインターネット グループ管理プロトコル (IGMP) プロファイルをインターフェイスに適用することにより、1 つまたは複数の IP マルチキャスト グループに加入できるかどうかを制御するには、インターフェイス コンフィギュレーション モードで **ip igmp filter** コマンドを使用します。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

**ip igmp filter** *profile number*

**no ip igmp filter**

## 構文の説明

*profile number* 適用する IGMP プロファイル番号。指定できる範囲は 1 ~ 4294967295 です。

## コマンド デフォルト

IGMP のフィルタは適用されていません。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

IGMP フィルタはレイヤ 2 の物理インターフェイスだけに適用できます。ルーテッドポート、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 IGMP フィルタを適用することはできません。

IGMP のプロファイルは 1 つまたは複数のポート インターフェイスに適用できますが、1 つのポートに対して 1 つのプロファイルだけ適用できます。

## 例

次の例では、IGMP プロファイル 22 をポートに適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp filter 22
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

## 関連コマンド

| コマンド   | 説明  |
|--|---|
| <a href="#">ip igmp profile</a>                            | 指定された IGMP プロファイル番号を設定します。  |
| <a href="#">show ip dhcp snooping statistics</a>           | 指定された IGMP プロファイルの特性を表示します。   |
| <a href="#">show running-config interface interface-id</a> | 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 Software Command Reference, Release 15.0』を参照してください。 |

# 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、または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するには、インターフェイス コンフィギュレーション モードで **ip igmp max-groups** 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

|                       |   |
|-----------------------|---|
| <b>number</b>         | 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。デフォルト設定は無制限です。          |
| <b>action deny</b>    | 最大数のエントリが IGMP スヌーピング転送テーブルにある場合、次の IGMP Join 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。 |
| <b>action replace</b> | 最大数のエントリが IGMP スヌーピング転送テーブルにあるときに、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に置き換えます。         |

## コマンドデフォルト

デフォルトの最大グループ数は制限なしです。

インターフェイス上に IGMP グループ エントリの最大数があることをスイッチが学習した後の、デフォルトのスロットリングアクションでは、インターフェイスが受信する次の IGMP レポートをドロップし、インターフェイスに IGMP グループのエントリを追加しません。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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、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 IGMP 最大グループ数を設定することはできません。

IGMP スロットリング アクションを設定する場合には、次の注意事項に従ってください。

- スロットリング アクションを **deny** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れた後で、エントリの最大数が転送テーブルにある場合は、インターフェイス上で受信された次の IGMP レポートをスイッチがドロップします。
- スロットリング アクションを **replace** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは削除されます。最大数のエントリが転送テーブルにある場合、スイッチはランダムに選択したマルチキャスト エントリを受信した IGMP レポートと置き換えます。
- 最大グループ制限がデフォルト (制限なし) に設定されている場合、**ip igmp max-groups {deny | replace}** コマンドを入力しても無効です。

**例** 次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp max-groups 25
```

次の例では、最大数のエントリが転送テーブルにあるときに、IGMP レポートを受信した既存のグループを新しいグループと置き換えるように設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp max-groups action replace
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

#### 関連コマンド

| コマンド  | 説明   |
|---|--|
| <b>show running-config interface</b><br><i>interface-id</i> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、グローバル コンフィギュレーション モードで **ip igmp profile** コマンドを指定します。このモードで、スイッチポートからの IGMP メンバーシップ 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。

## コマンドデフォルト

IGMP プロファイルは定義されていません。設定された場合、デフォルトの IGMP プロファイルとの一致機能は、一致するアドレスを拒否する設定になります。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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することを指定します。これがデフォルトの状態です。
- **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することを指定します。
- **range** : プロファイルの 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
```

## 関連コマンド

| コマンド   | 説明   |
|--|--|
| <a href="#">ip igmp filter</a>                   | 指定のインターフェイスに対し、IGMP を適用します。                    |
| <a href="#">show ip dhcp snooping statistics</a> | 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

スイッチでインターネット グループ管理プロトコル (IGMP) スヌーピングをグローバルにまたは VLAN 単位でイネーブルにするには、グローバル コンフィギュレーション モードで **ip igmp snooping** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

**no ip igmp snooping [vlan vlan-id]**

## 構文の説明

**vlan vlan-id** (任意) 指定された VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。

## コマンドデフォルト

スイッチ上で、IGMP スヌーピングはグローバルにイネーブルです。  
VLAN インターフェイス上で、IGMP スヌーピングはイネーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、すべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

## 例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping
```

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1
```

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

## 関連コマンド

| コマンド  | 説明                                     |
|---|--|
| <a href="#">ip igmp snooping report-suppression</a> | IGMP レポート抑制をイネーブルにします。                 |
| <a href="#">show ip dhcp snooping statistics</a>    | スヌーピング設定を表示します。                        |
| <a href="#">show ip igmp snooping groups</a>        | IGMP スヌーピング マルチキャスト情報を表示します。           |
| <a href="#">show ip igmp snooping mrouter</a>       | IGMP スヌーピング ルータ ポートを表示します。             |
| <a href="#">show ip igmp snooping querier</a>       | 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

インターネット グループ管理プロトコル (IGMP) の設定可能な Leave タイマーをグローバルに、または VLAN 単位でイネーブルにするには、グローバル コンフィギュレーション モードで **ip igmp snooping last-member-query-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**ip igmp snooping [vlan *vlan-id*] last-member-query-interval *time***

**no ip igmp snooping [vlan *vlan-id*] last-member-query-interval**

## 構文の説明

|                            |   |
|----------------------------|---|
| <b>vlan <i>vlan-id</i></b> | (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。 |
| <b><i>time</i></b>         | 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。  |

## コマンド デフォルト

デフォルトのタイムアウト設定は 1000 ミリ秒です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 関連コマンド

| コマンド  | 説明                                    |
|---|---------------------------------------|
| <a href="#">ip igmp snooping</a>                      | 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。 |
| <a href="#">ip igmp snooping vlan immediate-leave</a> | IGMP 即時脱退処理をイネーブルにします。                |
| <a href="#">ip igmp snooping vlan mrouter</a>         | 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。    |
| <a href="#">ip igmp snooping vlan static</a>          | レイヤ 2 ポートをグループのメンバとして設定します。           |
| <a href="#">show ip igmp snooping</a>                 | IGMP スヌーピング設定を表示します。                  |

# ip igmp snooping querier

レイヤ 2 ネットワークのインターネット グループ管理プロトコル (IGMP) クエリア機能をグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで **ip igmp snooping querier** 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

|   |   |
|---|---|
| <b>vlan <i>vlan-id</i></b>                                      | (任意) 指定した 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。   |
| <b>address <i>ip-address</i></b>                                | (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。  |
| <b>max-response-time <i>response-time</i></b>                   | (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。   |
| <b>query-interval <i>interval-count</i></b>                     | (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。   |
| <b>tcn query[count <i>count</i>   interval <i>interval</i>]</b> | (任意) トポロジ変更通知 (TCN) 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"> <li><b>count <i>count</i></b> : 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。</li> <li><b>interval <i>interval</i></b> : TCN クエリー間隔を設定します。指定できる範囲は 1 ~ 255 です。</li> </ul> |
| <b>timer expiry</b>   | (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。   |
| <b>version <i>version</i></b>                                   | (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。  |

## コマンド デフォルト

IGMP スヌーピング クエリア機能は、スイッチでグローバルにイネーブルです。

イネーブルになっている場合、マルチキャスト対応デバイスから IGMP トラフィックを検出すると、IGMP スヌーピング クエリアはディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**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す。デバイスが IGMPv1 を使用している場合は、**max-response-time** を設定できません (値を設定できず、0 に設定されています)。

IGMPv1 を実行している RFC に準拠していないデバイスは、**max-response-time** 値としてゼロ以外の値を持つ IGMP 一般クエリー メッセージを拒否することがあります。デバイスで IGMP 一般クエリー メッセージを受け入れる場合、IGMP スヌーピング クエリアが IGMPv1 を実行するように設定します。

VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

**例**

次の例では、IGMP スヌーピング クエリア機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping querier
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

次の例では、IGMP スヌーピング クエリアの時間間隔を 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier query-interval 60
```

次の例では、IGMP スヌーピング クエリアの TCN クエリー カウントを 25 に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier tcn count 25
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier timeout expiry 60
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier version 2
```

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

**関連コマンド**

| コマンド  | 説明                           |
|---|------------------------------|
| <a href="#">ip igmp snooping report-suppression</a> | IGMP レポート抑制をイネーブルにします。       |
| <a href="#">show ip igmp snooping</a>               | IGMP スヌーピング設定を表示します。         |
| <a href="#">show ip igmp snooping groups</a>        | IGMP スヌーピング マルチキャスト情報を表示します。 |
| <a href="#">show ip igmp snooping mrouter</a>       | IGMP スヌーピング ルータ ポートを表示します。   |

# ip igmp snooping report-suppression

インターネット グループ管理プロトコル (IGMP) レポート抑制をイネーブルにするには、グローバル コンフィギュレーション モードで **ip igmp snooping report-suppression** 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。

## コマンドデフォルト

IGMP レポート抑制はイネーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 関連コマンド

| コマンド                                  | 説明                                    |
|---------------------------------------|---------------------------------------|
| <a href="#">ip igmp snooping</a>      | 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。 |
| <a href="#">show ip igmp snooping</a> | 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

インターネット グループ管理プロトコル (IGMP) トポロジ変更通知 (TCN) の動作を設定するには、グローバル コンフィギュレーション モードで **ip igmp snooping tcn** コマンドを使用します。デフォルト設定に戻すには、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

|                                |   |
|--------------------------------|---|
| <b>flood query count count</b> | 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。             |
| <b>query solicit</b>           | 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。 |

## コマンド デフォルト

TCN フラッド クエリー カウントは 2 です。

TCN クエリー要求はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

TCN イベント後にマルチキャスト トラフィックがフラッディングする時間を制御するには、**ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。**ip igmp snooping tcn flood query count** コマンドを使用して TCN フラッド クエリー カウントを 1 に設定した場合、1 つの一般的クエリーの受信後にフラッディングが停止します。カウントを 7 に設定すると、TCN イベントによるマルチキャスト トラフィックのフラッディングは、7 つの一般的クエリーを受信するまで続きます。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せん。

スパニングツリー ルートかどうかにかかわらず、グローバル Leave メッセージを送信するようにスイッチをイネーブルにするには、**ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。また、このコマンドは、TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げます。

## 例

次の例では、マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を 7 に指定する方法を示します。

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

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

## 関連コマンド

| コマンド                                       | 説明   |
|--|--|
| <a href="#">ip igmp snooping</a>           | 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。                  |
| <a href="#">ip igmp snooping tcn flood</a> | 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。 |
| <a href="#">show ip igmp snooping</a>      | スイッチまたは VLAN の IGMP スヌーピング設定を表示します。                    |

# ip igmp snooping tcn flood

マルチキャスト フラッディングをインターネット グループ管理プロトコル (IGMP) スヌーピング スパニングツリー トポロジ変更通知 (TCN) の動作として設定するには、インターフェイス コンフィギュレーション モードで **ip igmp snooping tcn flood** コマンドを使用します。マルチキャスト フラッディングをディセーブルにするには、このコマンドの **no** 形式を使用します。

**ip igmp snooping tcn flood**

**no ip igmp snooping tcn flood**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

マルチキャスト フラッディングは、スパニングツリー TCN のイベント中、インターフェイス上でイネーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 Traffic はすべてのポートに対してフラッディングします。異なるマルチキャスト グループに加入している接続ホストを持つポートがスイッチに多数ある場合、フラッディングがリンクの容量を超過し、パケット損失を招くことがあります。

**ip igmp snooping tcn flood query count count** グローバル コンフィギュレーション コマンドを使用して、フラッディング クエリー カウントを変更できます。

## 例

次の例では、インターフェイス上でマルチキャスト フラッディングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no ip igmp snooping tcn flood
```

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

## 関連コマンド

| コマンド                                  | 説明                                    |
|---------------------------------------|---------------------------------------|
| <a href="#">ip igmp snooping</a>      | 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。 |
| <a href="#">ip igmp snooping tcn</a>  | スイッチで IGMP TCN 動作を設定します。              |
| <a href="#">show ip igmp snooping</a> | 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 単位で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、グローバル コンフィギュレーション モードで **ip igmp snooping immediate-leave** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**ip igmp snooping vlan *vlan-id* immediate-leave**

**no ip igmp snooping vlan *vlan-id* immediate-leave**

## 構文の説明

*vlan-id* IGMP および即時脱退をイネーブルにする特定の VLAN。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。

## コマンド デフォルト

IGMP の即時脱退処理はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

VLAN の各ポート上で 1 つのレシーバの最大値が設定されている場合に限り、即時脱退処理の機能を設定してください。設定は、NVRAM 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 が稼働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                                     |
|---|--|
| <a href="#">ip igmp snooping report-suppression</a> | IGMP レポート抑制をイネーブルにします。                 |
| <a href="#">show ip igmp snooping</a>               | スヌーピング設定を表示します。                        |
| <a href="#">show ip igmp snooping groups</a>        | IGMP スヌーピング マルチキャスト情報を表示します。           |
| <a href="#">show ip igmp snooping mrouter</a>       | IGMP スヌーピング ルータ ポートを表示します。             |
| <a href="#">show ip igmp snooping querier</a>       | 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するには、グローバル コンフィギュレーション モードで **ip igmp snooping vlan mrouter** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp | pim-dvmrp}}
```

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

## 構文の説明

|   |  |
|---|--|
| <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。  |
| <b>interface</b> <i>interface-id</i>            | マルチキャスト ルータへのネクスト ホップ インターフェイスを指定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>fastethernet</b> <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。</li> <li><b>gigabitethernet</b> <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。</li> <li><b>port-channel</b> <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 ~ 6 です。</li> </ul> |
| <b>learn</b> { <b>cgmp</b>   <b>pim-dvmrp</b> } | マルチキャスト ルータの学習方式を指定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>cgmp</b> : Cisco Group Management Protocol (CGMP) パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するように設定します。</li> <li><b>pim-dvmrp</b> : 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) パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するように設定します。</li> </ul>                   |

## コマンドデフォルト

デフォルトでは、マルチキャスト ルータ ポートはありません。

デフォルトの学習方式は **pim-dvmrp** です。IGMP クエリーおよび PIM-DVMRP パケットをスヌーピングします。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

CGMP の学習方式は制御トラフィックの削減に役立ちます。

設定は、NVRAM に保存されます。

#### 例

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/1
```

次の例では、マルチキャスト ルータの学習方式を CGMP として指定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
```

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

#### 関連コマンド

| コマンド                                       | 説明                                     |
|--|--|
| <b>ip igmp snooping report-suppression</b> | IGMP レポート抑制をイネーブルにします。                 |
| <b>show ip igmp snooping</b>               | スヌーピング設定を表示します。                        |
| <b>show ip igmp snooping groups</b>        | IGMP スヌーピング マルチキャスト情報を表示します。           |
| <b>show ip igmp snooping mrouter</b>       | IGMP スヌーピング ルータ ポートを表示します。             |
| <b>show ip igmp snooping querier</b>       | 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、マルチキャスト グループのメンバとしてレイヤ 2 ポートを追加するには、グローバル コンフィギュレーション モードで **ip igmp snooping static** 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

|                                      |  |
|--------------------------------------|--|
| <b><i>vlan-id</i></b>                | 特定の VLAN の 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。   |
| <b><i>ip-address</i></b>             | 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。  |
| <b>interface <i>interface-id</i></b> | 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"> <li><b>fastethernet <i>interface number</i></b> : ファストイーサネット IEEE 802.3 インターフェイス。</li> <li><b>gigabitethernet <i>interface number</i></b> : ギガビットイーサネット IEEE 802.3z インターフェイス。</li> <li><b>port-channel <i>interface number</i></b> : チャネル インターフェイス。指定できる範囲は 0 ~ 6 です。</li> </ul> |

## コマンド デフォルト

デフォルトでは、マルチキャスト グループのメンバとしてスタティックに設定されたポートはありません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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、インターフェイス上のホストをスタティックに設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface gigabitethernet1/1
Configuring port gigabitethernet1/1 on group 0100.5e02.0203
```

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

## 関連コマンド

| コマンド  | 説明                                     |
|---|--|
| <a href="#">ip igmp snooping report-suppression</a> | IGMP レポート抑制をイネーブルにします。                 |
| <a href="#">show ip igmp snooping</a>               | スヌーピング設定を表示します。                        |
| <a href="#">show ip igmp snooping groups</a>        | IGMP スヌーピング マルチキャスト情報を表示します。           |
| <a href="#">show ip igmp snooping mrouter</a>       | IGMP スヌーピング ルータ ポートを表示します。             |
| <a href="#">show ip igmp snooping querier</a>       | 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 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、グローバル コンフィギュレーション モードで **ip source binding** 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

|                                      |  |
|--------------------------------------|--|
| <i>mac-address</i>                   | MAC アドレスを指定します。                        |
| <b>vlan</b> <i>vlan-id</i>           | VLAN 番号を指定します。有効な範囲は 1 ~ 4094 です。      |
| <i>ip-address</i>                    | IP アドレスを指定します。                         |
| <b>interface</b> <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。 |

## コマンド デフォルト

IP 送信元バインディングは設定されていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

スタティック IP 送信元バインディング エントリには、IP アドレス、関連付けられた MAC アドレス、および関連付けられた VLAN 番号が含まれます。エントリは、MAC アドレスおよび VLAN 番号に基づいています。IP アドレスだけの変更でエントリを変更する場合は、スイッチは新しいエントリを作成せずに、エントリを更新します。

## 例

次の例では、スタティック IP 送信元バインディングを追加する方法を示します。

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface gigabitethernet1/1
```

次の例では、スタティック バインディングを追加してから、その IP アドレスを変更する方法を示します。

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface gigabitethernet1/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface gigabitethernet1/1
```

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

## 関連コマンド

| コマンド                                   | 説明   |
|--|--|
| <a href="#">ip verify source</a>       | 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。            |
| <a href="#">show ip source binding</a> | スイッチ上の IP 送信元バインディングを表示します。                |
| <a href="#">show ip verify source</a>  | 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

セキュア シェル (SSH) Version 1 または SSH Version 2 を実行するようにスイッチを設定するには、グローバル コンフィギュレーション モードで **ip ssh** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**ip ssh version [1 | 2]**

**no ip ssh version [1 | 2]**

## 構文の説明

- |   |   |
|---|---|
| 1 | (任意) スイッチが SSH バージョン 1 (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。 |

## コマンド デフォルト

デフォルトのバージョンは、SSH クライアントでサポートされる最新の SSH バージョンです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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   |
|--------------------|--|
| <b>show ip ssh</b> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show ssh</b>    | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』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)

スイッチ仮想インターフェイス (SVI) またはレイヤ 3 インターフェイス上で sticky アドレス解決プロトコル (ARP) をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip sticky-arp** 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**



(注)

このコマンドは IP サービス イメージが実行されているスイッチ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。

## コマンド デフォルト

sticky ARP は、レイヤ 3 インターフェイスおよび標準 SVI 上でディセーブルになります。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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せん。

- レイヤ 3 インターフェイス
- 標準 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。
- 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
```

## ■ ip sticky-arp (インターフェイス コンフィギュレーション)

- 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   |
|-----------------|--|
| <b>arp</b>      | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show arp</b> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。   |

# ip verify source

インターフェイス上で 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 コンフィギュレーション モードで **ip verify source** コマンドを使用します。IP ソース ガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

**ip verify source [port-security]**

**no ip verify source**

## 構文の説明

**port-security** (任意) IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにします。

**port-security** キーワードを入力しない場合、IP アドレス フィルタリングによる IP ソース ガードがイネーブルになります。

## コマンド デフォルト

IP 送信元ガードはディセーブルです。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用します。

送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、インターフェイスのポートセキュリティをイネーブルにする必要があります。

## 例

次の例では、送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source
```

次の例では、送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source port-security
```

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

## ■ ip verify source

| 関連コマンド | コマンド                                  | 説明   |
|--------|---------------------------------------|--|
|        | <a href="#">ip source binding</a>     | スイッチにスタティック バインディングを設定します。                 |
|        | <a href="#">show ip verify source</a> | 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 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、インターフェイス コンフィギュレーション モードで **ipv6 address dhcp** 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、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

## 構文の説明

**rapid-commit** (任意) アドレス割り当てに 2 つのメッセージ交換方式を許可します。

## コマンドデフォルト

なし

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

**ipv6 address dhcp** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスは DHCP プロトコルを使用して IPv6 アドレスを動的に学習できます。

**rapid-commit** キーワードは、アドレス割り当ておよびその他の設定について、2 つのメッセージ交換を使用できるようにします。これをイネーブルにすると、クライアントは送信請求メッセージに **rapid-commit** オプションを含めます。

## 例

次の例では、IPv6 アドレスを要求して、**rapid-commit** オプションをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/3
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# ipv6 address dhcp rapid-commit
```

設定を確認するには、**show ipv6 dhcp interface** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                            | 説明  |
|---------------------------------|---|
| <b>show ipv6 dhcp interface</b> | DHCPv6 インターフェイスの情報を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# ipv6 dhcp client request vendor

IPv6 クライアントを Dynamic Host Configuration Protocol for IPv6 (DHCPv6) サーバのオプションを要求するように設定するには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp client request** 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、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

なし

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

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

ベンダー固有オプションを要求するには、**ipv6 dhcp client request vendor** インターフェイス コンフィギュレーション コマンドを使用します。イネーブルにすると、IPv6 アドレスを DHCP から取得するときだけこのコマンドの確認が行われます。インターフェイスが IPv6 アドレスを取得した後でこのコマンドを入力しても、次回クライアントが DHCP から IPv6 アドレスを取得するまでこのコマンドは有効になりません。

## 例

次の例では、ベンダー固有オプションの要求をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/3
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# ipv6 dhcp client request vendor-specific
```

## 関連コマンド

| コマンド                              | 説明                                |
|-----------------------------------|-----------------------------------|
| <a href="#">ipv6 address dhcp</a> | DHCP からインターフェイスの IPv6 アドレスを取得します。 |

# ipv6 dhcp ping packets

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) サーバが ping 操作の一部としてプールアドレスに送信するパケットの数を指定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp ping packets** 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、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

## 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。 |
|---------------|---|

## コマンドデフォルト

デフォルトは 0 です。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

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

DHCPv6 サーバは、要求元クライアントにアドレスを割り当てる前にプールアドレスに ping を送信します。ping の応答がない場合、サーバはアドレスが使用されていない可能性が高いと想定し、アドレスを要求元クライアントに割り当てます。

*number* 引数を 0 に設定すると、DHCPv6 サーバの ping 操作がオフになります。

## 例

次の例では、DHCPv6 サーバによる 2 回の ping 試行を指定する方法を示します（その後、ping 試行を停止します）。

```
Switch(config)# ipv6 dhcp ping packets 2
```

## 関連コマンド

| コマンド                                  | 説明   |
|---------------------------------------|--|
| <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、グローバル コンフィギュレーション モードで **ipv6 dhcp pool** コマンドを使用します。デフォルト設定に戻すには、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、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

## 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 (Engineering など) または整数 (0 など) を使用できます。 |
|-----------------|--|

## コマンドデフォルト

なし

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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

**ipv6 dhcp pool** コマンドは、DHCPv6 プール コンフィギュレーション モードをイネーブルにします。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **address prefix IPv6-prefix** : アドレス割り当てのアドレス プレフィックスを設定します。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。
- **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** : リンクアドレスの 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、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。

- **vendor-specific** : 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。使用できるコンフィギュレーション コマンドは、次のとおりです。
  - **vendor-id** : ベンダー固有の ID 番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ~ 4294967295 です。
  - **suboption number** : ベンダー固有のサブオプション番号を設定します。指定できる範囲は 1 ~ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプション パラメータで定義されているように入力します。

DHCPv6 設定情報プールを作成してから、**ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用してプールとインターフェイス上のサーバを関連付けます。ただし、情報プールを設定しない場合は、**ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用して DHCPv6 サーバ機能をインターフェイスでイネーブルにする必要があります。

DHCPv6 プールとインターフェイスを関連付けると、関連付けられているインターフェイス上の要求を処理するのはそのプールだけとなります。プールは、他のインターフェイスについても処理を行います。DHCPv6 プールとインターフェイスを関連付けない場合は、すべてのインターフェイスに対する要求を処理できます。

IPv6 アドレス プレフィックスを使用しないということは、プールは設定されているオプションだけを返すことを指します。

**link-address** キーワードを使用すると、必ずしもアドレスを割り当てなくてもリンク アドレスの照合を行うことができます。プール内の複数のリンク アドレス コンフィギュレーション コマンドを使用して、複数のリレーのプールを照合できます。

アドレス プール情報またはリンク情報のいずれかについて最長一致が行われるため、あるプールについてはアドレスを割り当てるように設定して、サブプレフィッ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 プレフィッ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 プレフィックスおよび 1 つの IPv6 アドレス プレフィッ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  |
|----------------------------------|---|
| <a href="#">ipv6 dhcp server</a> | インターフェイスで DHCPv6 サービスをイネーブルにします。  |
| <b>show ipv6 dhcp pool</b>       | DHCPv6 設定プールの情報を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、インターフェイス コンフィギュレーション モードで **ipv6 dhcp server** コマンドを使用します。インターフェイスで DHCPv6 サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ipv6 dhcp server [poolname | automatic] [rapid-commit] [preference value] [allow-hint]
```

```
no ipv6 dhcp server [poolname | automatic] [rapid-commit] [preference value] [allow-hint]
```



(注)

このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

## 構文の説明

|                         |   |
|-------------------------|---|
| <b>poolname</b>         | (任意) IPv6 DHCP プールのユーザ定義名。プール名には象徴的な文字列 (Engineering など) または整数 (0 など) を使用できます。                        |
| <b>automatic</b>        | (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。  |
| <b>rapid-commit</b>     | (任意) 2 つのメッセージ交換方式を許可します。   |
| <b>preference value</b> | (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を指定します。有効な範囲は 0 ~ 255 です。デフォルトのプリファレンス値は 0 です。 |
| <b>allow-hint</b>       | (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。                        |

## コマンド デフォルト

デフォルトでは、DHCPv6 パケットはインターフェイス上で処理されません。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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** キーワードは、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。サーバが IPv6 DHCP パケットを受信すると、サーバはそのパケットを DHCP リレーから受信したか、クライアントから直接受信したかを判別します。リレーからパケットを受信した場合、サーバは、クライアントに最も近い最初のリレーと関連付けられているパケット内部のリンク アドレス フィールドを確認します。サーバは、このリンク アドレスと、すべてのアドレス プレフィックスおよび IPv6 DHCP プールのリンク アドレス設定とを照合して、最長のプレフィッ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ックス照合を選択します。

**rapid-commit** キーワードは、2 つのメッセージ交換を使用できるようにします。

**preference** キーワードを 0 以外の値とともに設定すると、サーバはプリファレンス オプションを追加して、アドバタイズ メッセージのプリファレンス値を伝送します。この動作は、クライアントによるサーバの選択に影響を与えます。プリファレンス オプションを含まないアドバタイズ メッセージのプリファレンス値は 0 であると見なされます。クライアントが、プリファレンス値が 255 であるアドバタイズ メッセージを受信する場合、クライアントはメッセージの送信元であるサーバに要求メッセージを即時に送信します。

**allow-hint** キーワードを指定する場合、サーバは送信請求メッセージおよび要求メッセージの有効なクライアント提案アドレスを割り当てます。プレフィックス アドレスは、関連付けられているローカルプレフィックス アドレス プール内にあり、デバイスに割り当てられていない場合は有効です。

**allow-hint** キーワードを指定しない場合、サーバはクライアント ヒントを無視して、プール内のフリー リストにあるアドレスが割り当てられます。

DHCPv6 クライアント、サーバ、およびリレーの機能は、インターフェイス上で相互排他的です。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  |
|---------------------------------|---|
| <b>ipv6 dhcp pool</b>           | 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。   |
| <b>show ipv6 dhcp interface</b> | DHCPv6 インターフェイスの情報を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# ipv6 mld snooping

IP version 6 (IPv6) マルチキャストリスナー検出 (MLD) スヌーピングをグローバルにイネーブルにするか、または指定した VLAN でイネーブルにするには、キーワードを指定せずにグローバル コンフィギュレーション モードで **ipv6 mld snooping** コマンドを使用します。MLD スヌーピングを、スイッチ、スイッチ スタック、または VLAN 上でディセーブルにするには、このコマンドの **no** 形式を使用します。

**ipv6 mld snooping** [vlan *vlan-id*]

**no ipv6 mld snooping** [vlan *vlan-id*]



(注)

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

## 構文の説明

|                            |  |
|----------------------------|--|
| <b>vlan</b> <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。 |
|----------------------------|--|

## コマンド デフォルト

スイッチ上で、MLD スヌーピングはグローバルにディセーブルです。

すべての VLAN で MLD スヌーピングはイネーブルです。ただし、VLAN スヌーピングが実行される前に、MLD スヌーピングをグローバルにイネーブルにする必要があります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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   |
|-------------------------------|--|
| <b>sdm prefer</b>             | 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。 |
| <b>show ipv6 mld snooping</b> | MLD スヌーピング設定を表示します。                              |

# ipv6 mld snooping last-listener-query-count

クライアントが期限切れになる前に送信される IP version 6 (IPv6) マルチキャストリスナー検出 Multicast Address Specific Query (MASQ) またはクエリーを設定するには、グローバル コンフィギュレーション モードで **ipv6 mld snooping last-listener-query-count** コマンドを使用します。クエリー カウントをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

**ipv6 mld snooping [vlan *vlan-id*] last-listener-query-count *integer\_value***

**no ipv6 mld snooping [vlan *vlan-id*] last-listener-query-count**



(注)

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

## 構文の説明

|                             |   |
|-----------------------------|---|
| <b>vlan <i>vlan-id</i></b>  | (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。 |
| <b><i>integer_value</i></b> | 指定できる範囲は 1 ~ 7 です。  |

## コマンド デフォルト

デフォルトのグローバル カウントは 2 です。  
デフォルトの VLAN カウントは 0 です (グローバル カウントを使用します)。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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応答できます (IGMP Leave メッセージに相当)。即時脱退が設定されていない場合 (1 つのグループに対し複数のクライアントが同じポート上に存在する場合は設定しない)、設定された last-listener クエリー カウントにより、MLD クライアントが期限切れになる前に送信する MASQ の数が決定します。

VLAN に last-listener クエリー カウントを設定した場合、グローバルに設定された値より優先されません。VLAN の数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、グローバルな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   |
|--|--|
| <a href="#">ipv6 mld snooping last-listener-query-interval</a> | IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。      |
| <a href="#">sdm prefer</a>                                     | 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。 |
| <a href="#">show ipv6 mld snooping querier</a>                 | 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 上の IP version 6 (IPv6) マルチキャストリスナー検出 (MLD) スヌーピングの last-listener クエリー間隔を設定するには、グローバル コンフィギュレーション モードの **ipv6 mld snooping last-listener-query-interval** コマンドを使用します。この時間間隔は、Multicast Address Specific Query (MASQ) マルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する最大時間です。クエリー時間をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

```
ipv6 mld snooping [vlan vlan-id] last-listener-query-interval integer_value
```

```
no ipv6 mld snooping [vlan vlan-id] last-listener-query-interval
```



(注)

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

## 構文の説明

|                             |   |
|-----------------------------|---|
| <b>vlan <i>vlan-id</i></b>  | (任意) 指定の VLAN で last-listener クエリー間隔を設定します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。                        |
| <b><i>integer_value</i></b> | MASQ を発行した後マルチキャスト グループからポートを削除するまでにマルチキャスト ルータが待機する時間 (1000 秒単位)。指定できる範囲は 100 ~ 32,768 です。デフォルト値は 1000 (1 秒) です。 |

## コマンド デフォルト

デフォルトのグローバル クエリー間隔 (最大応答時間) は 1000 (1 秒) です。  
デフォルトの VLAN クエリー間隔 (最大応答時間) は 0 です (グローバル カウントが使用されます)。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 アドレスのメンバーシップ 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   |
|---|--|
| <a href="#">ipv6 mld snooping last-listener-query-count</a> | IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。   |
| <a href="#">sdm prefer</a>                                  | 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。 |
| <a href="#">show ipv6 mld snooping querier</a>              | 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) マルチキャスト リスナー検出 (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、グローバル コンフィギュレーション モードで **ipv6 mld snooping listener-message-suppression** コマンドを使用します。MLD スヌーピング リスナー メッセージ抑制をディセーブルにするには、このコマンドの **no** 形式を使用します。

**ipv6 mld snooping listener-message-suppression**

**no ipv6 mld snooping listener-message-suppression**



(注)

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

## コマンドデフォルト

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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  |
|--|---|
| <a href="#">ipv6 mld snooping</a>      | IPv6 MLD スヌーピングをイネーブルにします。                        |
| <a href="#">sdm prefer</a>             | 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に SDM テンプレートを設定します。 |
| <a href="#">show ipv6 mld snooping</a> | 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前にスイッチが送信する IP version 6 (IPv6) マルチキャスト リスナー 検出 (MLD) クエリーの数を設定するか、または VLAN ID を入力して VLAN 単位でクエリーの数を設定するには、グローバル コンフィギュレーション モードで **ipv6 mld snooping robustness-variable** コマンドを使用します。変数をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

**ipv6 mld snooping [vlan *vlan-id*] robustness-variable *integer\_value***

**no ipv6 mld snooping [vlan *vlan-id*] robustness-variable**



(注)

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

## 構文の説明

|                             |   |
|-----------------------------|---|
| <b>vlan <i>vlan-id</i></b>  | (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。 |
| <b><i>integer_value</i></b> | 指定できる範囲は 1 ~ 3 です。  |

## コマンド デフォルト

デフォルトのグローバル ロバストネス変数 (リスナーを削除する前のクエリー数) は、2 です。  
デフォルトの VLAN ロバストネス変数 (マルチキャスト アドレスが期限切れになる前のクエリー数) は 0 です。リスナーの期限の判断には、グローバル ロバストネス変数が使用されます。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## ■ ipv6 mld snooping robustness-variable

## 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   |
|---|--|
| <a href="#">ipv6 mld snooping last-listener-query-count</a> | IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。   |
| <a href="#">sdm prefer</a>                                  | 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。 |
| <a href="#">show ipv6 mld snooping</a>                      | MLD スヌーピング設定を表示します。                              |

# ipv6 mld snooping tcn

IP version 6 (IPv6) マルチキャストリスナー検出 (MLD) トポロジ変更通知 (TCN) 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 **ipv6 mld snooping tcn** コマンドを使用します。デフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

```
ipv6 mld snooping tcn {flood query count integer_value | query solicit}
```

```
no ipv6 mld snooping tcn {flood query count integer_value | query solicit}
```



(注)

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

## 構文の説明

|  |  |
|--|--|
| <b>flood query count</b><br><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。 |
| <b>query solicit</b>                             | TCN クエリーの送信請求をイネーブルにします。   |

## コマンド デフォルト

TCN クエリー送信請求はディセーブルです。  
イネーブルの場合、デフォルトのフラッディング クエリー カウントは 2 です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## ■ ipv6 mld snooping tcn

| 関連コマンド | コマンド                                   | 説明   |
|--------|--|--|
|        | <a href="#">sdm prefer</a>             | 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。 |
|        | <a href="#">show ipv6 mld snooping</a> | 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) マルチキャスト リスナー検出 (MLD) スヌーピングパラメータを設定するには、グローバル コンフィギュレーション モードで **ipv6 mld snooping vlan** コマンドを使用します。パラメータをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

```
ipv6 mld snooping vlan vlan-id [immediate-leave | mrouter interface interface-id | static
ipv6-multicast-address interface interface-id]
```

```
no ipv6 mld snooping vlan vlan-id [immediate-leave | mrouter interface interface-id | static
ip-address interface interface-id]
```



(注)

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

## 構文の説明

|   |  |
|---|--|
| <b>vlan</b> <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。  |
| <b>immediate-leave</b>                      | (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 <b>no</b> 形式を使用します。                  |
| <b>mrouter interface</b>                    | (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 <b>no</b> 形式を使用します。   |
| <b>static</b> <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。   |
| <b>interface</b> <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 <b>ポートチャネル</b> インターフェイスになることができます。 |

## コマンドデフォルト

MLD スヌーピング即時脱退処理はディセーブルです。  
デフォルトでは、スタティック IPv6 マルチキャスト グループは設定されていません。  
デフォルトでは、マルチキャスト ルータ ポートはありません。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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、Catalyst 3750 または Catalyst 3560 スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

1002 ~ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

## 例

次の例では、VLAN 1 で MLD 即時脱退処理をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、VLAN 1 で MLD 即時脱退処理をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、ポートをマルチキャスト ルータ ポートとして設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/01/2
```

次の例では、スタティック マルチキャスト グループを設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/01/2
```

設定を確認するには、**show ipv6 mld snooping vlan vlan-id** ユーザ EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                   | 説明  |
|--|---|
| <a href="#">ipv6 mld snooping</a>      | IPv6 MLD スヌーピングをイネーブルにします。                        |
| <a href="#">ipv6 mld snooping vlan</a> | VLAN で IPv6 MLD スヌーピングを設定します。                     |
| <a href="#">sdm prefer</a>             | 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に SDM テンプレートを設定します。 |
| <a href="#">show ipv6 mld snooping</a> | IPv6 MLD スヌーピング設定を表示します。                          |

# l2nat

選択したインターフェイスで1つ以上の VLAN にレイヤ 2 NAT インスタンスを適用するには、インターフェイス コンフィギュレーション モードで **l2nat** コマンドを入力します。

VLAN または VLAN 範囲からレイヤ 2 NAT インスタンスを削除するには、このコマンドの **no** 形式を入力します。

```
l2nat instance_name [vlan | vlan_range]
```

```
no l2nat instance_name [vlan | vlan_range]
```

| 構文の説明                | 説明  |
|----------------------|---|
| <i>instance_name</i> | 選択したインターフェイスに適用するレイヤ 2 NAT インスタンス                           |
| <i>vlan</i>          | (任意) VLAN または VLAN 範囲が含まれていない場合、インスタンスはタグなしトラフィックだけに適用されます。 |
| <i>vlan_range</i>    | (任意) VLAN または VLAN 範囲が含まれていない場合、インスタンスはタグなしトラフィックだけに適用されます。 |

コマンド デフォルト なし

コマンド モード インターフェイス コンフィギュレーション

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(2)EB | このコマンドが導入されました。 |

## 使用上のガイドライン

- デフォルトの VLAN はネイティブ VLAN です。
- 同じインスタンスをタグなしおよびタグ付きトラフィックに適用する必要がある場合 (ネイティブ VLAN の場合)、明示的に両方の VLAN にインスタンスを適用する必要があります。
- VLAN あたりレイヤ 2 NAT インスタンスを1つだけ指定できますが、同じ変換を再利用するために複数の VLAN に同じインスタンスを適用できます。
- このコマンドは、ギガビット アップリンク インターフェイスだけに使用できます。
- EtherChannel に2つのアップリンク ポートを設定してから、1つのポートにインスタンスを適用すると、同じインスタンスがもう1つのポートにも適用されます。統計情報では、両方のポートの番号は、EtherChannel 用に結合され、報告されます。
- ポートが呼び出し音モードに設定されている場合、同じ VLAN およびインターフェイスの組み合わせに同じインスタンスを適用する必要があります。統計情報は、アップリンク ポートごとに報告されます。

例 次に Instance1 という名前のインスタンスを VLAN 10 に適用する例を示します。

```
Switch(config)# interface Gi1/1
Switch(config-if)# l2nat Instance1 10
```

この例では、インスタンスをネイティブ VLAN に適用します。

```
Switch(config)# interface Gi1/1
Switch(config-if)# l2nat Instance1
```

#### 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">inside from</a>                     | レイヤ 2 NAT を使用して内部アドレスを外部アドレスに変換します。                         |
| <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">outside from</a>                    | レイヤ 2 NAT を使用して、外部アドレスを内部アドレスに変換します。                        |
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                           |
| <a href="#">show l2nat interface</a>            | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。                |
| <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# I2nat instance

レイヤ 2 NAT インスタンスを作成またはレイヤ 2 NAT インスタンスを設定するサブモードを開始するには、グローバル コンフィギュレーション モードで **l2nat instance** コマンドを使用します。レイヤ 2 NAT 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。

**l2nat instance *instance\_name***

**no l2nat instance *instance\_name***

## 構文の説明

*instance\_name* このレイヤ 2 NAT インスタンスを識別する文字列

## コマンド デフォルト

なし

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(2)EB | このコマンドが導入されました。 |

## 使用上のガイドライン

- インスタンスの最大数は 128 です。
- VLAN ごとの変換エントリ数に制限はありません。

## 例

次に Instance1 という名前の新しい l2nat インスタンスを作成する例を示します。この同じコマンドをこのインスタンスのサブモードを開始させるために使用できます。

```
Switch(config)# l2nat instance Instance1
```

次に Instance1 という名前の l2nat インスタンスを削除する例を示します。

```
Switch(config)# no l2nat instance Instance1
```

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">debug l2nat</a>                       | 設定を適用する場合にリアルタイムでレイヤ 2 NAT の設定の詳細を表示します。               |
| <a href="#">fixup</a>                             | 指定したレイヤ 2 NAT インスタンスのプロトコルのフィックスアップをイネーブルにします。         |
| <a href="#">inside from</a>                       | レイヤ 2 NAT を使用して内部アドレスを外部アドレスに変換します。                    |
| <a href="#">l2nat</a>                             | 選択したインターフェイスの 1 つまたはすべての VLAN にレイヤ 2 NAT インスタンスを適用します。 |
| <a href="#">outside from</a>                      | レイヤ 2 NAT を使用して、外部アドレスを内部アドレスに変換します。                   |
| <a href="#">permit (config-l2nat コンフィギュレーション)</a> | 変換するように設定されていない指定したタイプのトラフィックを許可またはブロックします。            |

| コマンド  | 説明   |
|---|--|
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。            |
| <a href="#">show l2nat interface</a>            | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。 |
| <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。           |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。           |

# 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、インターフェイス コンフィギュレーション モードで **lacp port-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**lacp port-priority priority**

**no lacp port-priority**

## 構文の説明

*priority* LACP のポート プライオリティ。指定できる範囲は 1 ~ 65535 です。

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**lacp port-priority** インターフェイス コンフィギュレーション コマンドは、LACP チャネル グループに 9 つ以上のポートがある場合、バンドルされるポートと、ホットスタンバイ モードに置かれるポートを判別します。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。

ポート プライオリティの比較では、数値が小さいほどプライオリティが高くなります。LACP チャネル グループに 9 つ以上のポートがある場合、LACP ポート プライオリティの数値が小さい（つまり、高いプライオリティ値の）8 つのポートがチャネル グループにバンドルされ、それより低いプライオリティのポートはホットスタンバイ モードに置かれます。LACP ポート プライオリティが同じポートが 2 つ以上ある場合（たとえば、そのいずれもデフォルト設定の 65535 に設定されている場合）、ポート番号の内部値によりプライオリティが決定します。



(注)

LACP リンクを制御するスイッチ上にポートがある場合に限り、LACP ポート プライオリティは有効です。リンクを制御するスイッチの判別については、**lacp system-priority** グローバル コンフィギュレーション コマンドを参照してください。

LACP ポート プライオリティおよび内部ポート番号値を表示するには、**show lacp internal** 特権 EXEC コマンドを使用します。

物理ポート上の LACP の設定に関する詳細については、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 (EtherChannel の設定)」の章を参照してください。

## ■ lacp port-priority

## 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 gigabitethernet1/1
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   |
|--|--|
| <b>channel-group</b>                             | EtherChannel グループにイーサネットポートを割り当てます。        |
| <b>lacp system-priority</b>                      | LACP システム プライオリティを設定します。                   |
| <b>show lacp [channel-group-number] internal</b> | 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、グローバル コンフィギュレーション モードで **lacp system-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**lacp system-priority** *priority*

**no lacp system-priority**

|            |                 |   |
|------------|-----------------|---|
| 構文の説明      | <i>priority</i> | 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。 |
| コマンド 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            | 変更内容                                      |
|            | 15.0(1)EY       | このコマンドが導入されました。                           |

**使用上のガイドライン** **lacp system-priority** コマンドでは、ポート プライオリティを制御する LACP リンクのスイッチが判別されます。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。LACP チャネル グループに 9 つ以上のポートがある場合、リンクの制御側終端にあるスイッチは、ポート プライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイ モードに置くポートを判別します。他のスイッチ上のポート プライオリティ（リンクの非制御側終端）は無視されます。

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。したがって、LACP システム プライオリティの数値が小さい（プライオリティ値の高い）システムが制御システムとなります。どちらのスイッチも同じ LACP システム プライオリティである場合（たとえば、どちらもデフォルト設定の 32768 が設定されている場合）、LACP システム ID（スイッチの MAC アドレス）により制御するスイッチが判別されます。

**lacp system-priority** コマンドは、スイッチ上のすべての LACP EtherChannel に適用されます。

ホットスタンバイ モード（ポート ステート フラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

物理ポート上の LACP の設定の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

**例** 次の例では、LACP のシステム プライオリティを設定する方法を示します。

```
Switch(config)# lacp system-priority 20000
```

## ■ lacp system-priority

## 関連コマンド

| コマンド                               | 説明                                   |
|------------------------------------|--------------------------------------|
| <a href="#">channel-group</a>      | EtherChannel グループにイーサネット ポートを割り当てます。 |
| <a href="#">lacp port-priority</a> | LACP ポート プライオリティを設定します。              |
| <a href="#">show lacp sys-id</a>   | LACP によって使用されるシステム識別子を表示します。         |

# link-diag error-rate

リンクの診断機能のウィンドウ サイズを設定するには、グローバル コンフィギュレーション モードで **link-diag error-rate** コマンドを使用します。

**link-diag error-rate (window-size {seconds})**

|       |                            |  |
|-------|----------------------------|--|
| 構文の説明 | <b>window-size seconds</b> | エラー レートの計算にリンクの診断エラー レート スライディング ウィンドウ期間を指定します。期間の範囲は 5 ~ 600 秒です。 |
|-------|----------------------------|--|

**コマンド デフォルト** デフォルトのウィンドウ サイズは 5 分です。

**コマンド モード** グローバル コンフィギュレーション

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン** エラー レートは時間のスライディング ウィンドウに基づいて計算されます。与えられたウィンドウ サイズについて、エラー パケット数とパケットの合計が、ウィンドウ期間内で 5 等分した時間でサンプリングされます。報告されたエラー レートは 5 つのサンプリングの平均であり、更新ごとにそのサイズの 5 分の 1 の期間でウィンドウがスライド (または更新) することを許可します。ウィンドウ サイズは秒単位で設定可能で、ウィンドウ サイズは 5 秒の倍数である必要があります。デフォルトのウィンドウに対応するサンプル レートは、1 分あたり 1 つのサンプルです。この結果、ウィンドウ サイズが変更されたインスタンスの後では、1 つのウィンドウ サイズの期間が経過するまで報告されるエラー レートは正確ではありません。

計算に使用されるカウンタは、**show interface counter** コマンドを使用してプラットフォーム カウンタから取得されます。受信方向について報告されたパケット エラーは、「アライメント エラー」、「FCS エラー」、「シンボル エラー」のフレーム エラー タイプです。送信方向について報告されたパケット エラーは、「過剰な衝突」、「過剰な遅延」のフレーム エラー タイプです。

**例** 次に、link-diag error-rate ウィンドウ サイズを 5 秒に設定する例を示します。

```
Switch(config)# link-diag error-rate window-size 5
```

| 関連コマンド | コマンド                                      | 説明                     |
|--------|---|------------------------|
|        | <a href="#">show interfaces counters</a>  | インターフェイス カウンタ情報を表示します。 |
|        | <a href="#">show link-diag error-rate</a> | エラー レート設定を表示します。       |

# link state group

リンクステート グループのメンバとしてポートを設定するには、インターフェイス コンフィギュレーション モードで **link state group** 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

|                   |   |
|-------------------|---|
| <b>number</b>     | (任意) リンクステート グループ番号。グループ番号は、1 ~ 6 です。     |
| <b>upstream</b>   | 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。 |
| <b>downstream</b> | 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。 |

## コマンドデフォルト

デフォルトのグループは group 1 です。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

指定されたリンク ステート グループのアップストリームまたはダウンストリーム インターフェイスとしてポートを設定するには、**link state group** インターフェイス コンフィギュレーション コマンドを使用します。グループ番号が省略されている場合、デフォルトのグループ番号は 1 です。

リンクステート トラッキングをイネーブルにするには、**link-state group** を作成し、リンクステート グループに割り当てるインターフェイスを指定します。ポートの集合 (EtherChannel)、アクセス モードまたはトランク モードの単一の物理ポート、またはルーテッド ポートをインターフェイスに指定できます。リンクステート グループでは、これらのインターフェイスはまとめてバンドルされます。ダウンストリーム インターフェイスは、アップストリーム インターフェイスにバインドされます。サーバに接続されたインターフェイスはダウンストリーム インターフェイスと呼ばれ、ディストリビューション スイッチおよびネットワーク装置に接続されたインターフェイスはアップストリーム インターフェイスと呼ばれます。

ダウンストリーム インターフェイスとアップストリーム インターフェイス間の連動の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels and Link-State Tracking」の章を参照してください。

設定上の問題を回避するために、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。
- インターフェイスは、複数のリンクステート グループのメンバにはなれません。
- スイッチ 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 gigabitethernet1/1 - 2  
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  |
|---------------------------------------|---|
| <a href="#">link state track</a>      | リンクステート グループをイネーブルにします。   |
| <a href="#">show link state group</a> | リンクステート グループ情報を表示します。   |
| <a href="#">show running-config</a>   | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、ユーザ EXEC モードで **link state track** 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。グループ番号は、1 ~ 6 です。デフォルトは 1 です。

## コマンドデフォルト

リンクステート トラッキングは、すべてのグループでディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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  |
|---------------------------------------|---|
| <a href="#">link state track</a>      | 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。  |
| <a href="#">show link state group</a> | リンクステート グループ情報を表示します。   |
| <a href="#">show running-config</a>   | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

## 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、グローバル コンフィギュレーション モードで **location** 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

|                       |   |
|-----------------------|---|
| <b>admin-tag</b>      | 管理タグまたはサイト情報を設定します。   |
| <b>civic-location</b> | 都市ロケーション情報を設定します。   |
| <b>elin-location</b>  | 緊急ロケーション情報 (ELIN) を設定します。   |
| <b>identifier id</b>  | 都市ロケーションまたは回線のロケーションの ID を指定します。指定できる ID 範囲は 1 ~ 4095 です。<br><br>(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。 |
| <i>string</i>         | 英数字形式のサイト情報またはロケーション情報。   |

### コマンド デフォルト

なし

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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
```

## ■ location (グローバル コンフィギュレーション)

```
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                       |
|--|--------------------------|
| <b>location</b> (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。 |
| <b>show location</b>                   | 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、インターフェイス モードで **location** 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

|  |  |
|--|--|
| <b>additional-location-information</b> | 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。  |
| <b>civic-location-id</b>               | 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。  |
| <b>elin-location-id</b>                | 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回線のロケーションの ID。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。 |

## コマンド デフォルト

なし

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**location civic-location-id id** インターフェイス コンフィギュレーション コマンドを入力すると、都市ロケーション コンフィギュレーション モードに入ります。このモードでは、追加のロケーション情報を入力することができます。

都市ロケーション ID は 250 バイトを超えてはなりません。

## 例

次の例では、インターフェイスに都市ロケーション情報を入力する方法を示します。

```
Switch(config-if) # interface gigabitethernet1/1
Switch(config-if) # location civic-location-id 1
Switch(config-if) # end
```

## ■ location (インターフェイス コンフィギュレーション)

次の例では、インターフェイスに緊急ロケーション情報を入力する方法を示します。

```
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# location elin-location-id 1
Switch(config-if)# end
```

## 関連コマンド

| コマンド                             | 説明                      |
|----------------------------------|-------------------------|
| <a href="#">link state group</a> | エンドポイントにロケーション情報を設定します。 |
| <a href="#">show location</a>    | 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、インターフェイス コンフィギュレーション モードで **logging event** 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

|                      |   |
|----------------------|---|
| <b>bundle-status</b> | BUNDLE および UNBUNDLE メッセージの通知をイネーブルにします。 |
| <b>link-status</b>   | 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。  |
| <b>spanning-tree</b> | スパニングツリー イベント通知をイネーブルにします。              |
| <b>status</b>        | 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。      |
| <b>trunk-status</b>  | 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。           |

## コマンドデフォルト

イベント ロギングはディセーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、スパニングツリー ロギングをイネーブルにする方法を示します。

```
Switch(config-if)# logging event spanning-tree
```

# logging event power-inline-status

Power over Ethernet (PoE) イベントのロギングをイネーブルにするには、**logging event power-inline-status** インターフェイス コンフィギュレーション コマンドを使用します。PoE ステータス イベントのロギ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。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

このコマンドには引数またはキーワードはありません。

## デフォルト

PoE イベントのロギングはイネーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース       | 変更内容            |
|------------|-----------------|
| 15.0(2)EY1 | このコマンドが導入されました。 |

## 使用上のガイドライン

**logging event power-inline-status** コマンドは、PoE インターフェイスでだけ使用できます。

## 例

次の例では、ポート上で PoE イベントのロギングをイネーブルにする方法を示します。

```
Switch(config-if)# interface fastEthernet 1/1
Switch(config-if)# logging event power-inline-status
Switch(config-if)#
```

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">power inline</a>                  | 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。 |
| <a href="#">show controllers power inline</a> | 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 パラメータを設定するには、グローバル コンフィギュレーション モードで **logging file** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**logging file** *filesystem:filename* [*max-file-size* | **nomax** [*min-file-size*]] [*severity-level-number* | *type*]

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

## 構文の説明

|                              |   |
|------------------------------|---|
| <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。<br><br>ローカル フラッシュ ファイル システムの構文<br><b>flash:</b>   |
| <i>max-file-size</i>         | (任意) ロギング ファイルの最大サイズ。指定できる範囲は 4096 ~ 2147483647 です。   |
| <b>nomax</b>                 | (任意) 最大ファイル サイズ (2147483647) を指定します。  |
| <i>min-file-size</i>         | (任意) ロギング ファイルの最小サイズ。指定できる範囲は 1024 ~ 2147483647 です。   |
| <i>severity-level-number</i> | (任意) ロギングの重大度レベル。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) ロギング タイプ。次のキーワードが有効です。 <ul style="list-style-type: none"> <li>• <b>emergencies</b> : システムは使用不可 (重大度 0)</li> <li>• <b>alerts</b> : 早急な対応が必要 (重大度 1)</li> <li>• <b>critical</b> : 危険な状態 (重大度 2)</li> <li>• <b>errors</b> : エラーが発生している状態 (重大度 3)</li> <li>• <b>warnings</b> : 警告状態 (重大度 4)</li> <li>• <b>notifications</b> : 通常ではあるが、重要なメッセージ (重大度 5)</li> <li>• <b>informational</b> : 通知メッセージ (重大度 6)</li> <li>• <b>debugging</b> : デバッグ メッセージ (重大度 7)</li> </ul> |

## コマンド デフォルト

ファイル サイズは最小で 2048 バイト、最大で 4096 バイトになります。  
デフォルトの重大度のレベルは 7 (**debugging** メッセージ : 数字的に低いレベル) です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**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、スイッチのコマンドライン インターフェイス (CLI) 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  |
|----------------------------|---|
| <b>show running-config</b> | 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 Software Command Reference, Release 15.0』を参照してください。 |

# mab request format attribute 32

スイッチ上で VLAN ID ベースの MAC 認証をイネーブルにするには、グローバル コンフィギュレーション モードで **mab request format attribute 32** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**mab request format attribute 32 vlan access-vlan**

**no mab request format attribute 32 vlan access-vlan**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

VLAN-ID ベースの MAC 認証はディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

RADIUS サーバがホスト MAC アドレスと VLAN に基づいて新しいユーザを認証できるようにするには、このコマンドを使用します。

Microsoft IAS RADIUS サーバを使用したネットワークでこのコマンドを使用します。Cisco ACS はこのコマンドを無視します。

## 例

次の例では、スイッチで VLAN-ID ベースの MAC 認証をイネーブルにする方法を示します。

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

## 関連コマンド

| コマンド                               | 説明   |
|------------------------------------|--|
| <b>authentication event</b>        | 特定の認証イベントのアクションを設定します。   |
| <b>authentication fallback</b>     | 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。 |
| <b>authentication host-mode</b>    | ポートで認証マネージャ モードを設定します。   |
| <b>authentication open</b>         | 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。                                  |
| <b>authentication order</b>        | ポートで使用する認証方式の順序を設定します。   |
| <b>authentication periodic</b>     | 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。  |
| <b>authentication port-control</b> | 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。  |
| <b>authentication priority</b>     | ポート プライオリティ リストに認証方式を追加します。  |
| <b>authentication timer</b>        | 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。                          |

| コマンド                            | 説明   |
|---------------------------------|--|
| <b>authentication violation</b> | 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。                                    |
| <b>mab</b>                      | ポートの MAC-based 認証をイネーブルにします。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。      |
| <b>mab eap</b>                  | 拡張認証プロトコル (EAP) を使用するようポートを設定します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show authentication</b>      | スイッチの認証マネージャ イベントに関する情報を表示します。   |

# mac access-group

レイヤ 2 インターフェイスに MAC アクセス コントロール リスト (ACL) を適用するには、インターフェイス コンフィギュレーション モードで **mac access-group** 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。   |
| <b>in</b>   | 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。 |

## コマンド デフォルト

MAC ACL は、インターフェイスには適用されません。

## コマンド モード

インターフェイス コンフィギュレーション (レイヤ 2 インターフェイスだけ)

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

MAC ACL は入力レイヤ 2 インターフェイスにだけ適用できます。レイヤ 3 インターフェイスには適用できません。

レイヤ 2 インターフェイスでは、IP アクセス リストを使用して IP トラフィックをフィルタリングし、MAC アクセス リストを使用して非 IP トラフィックをフィルタリングできます。インターフェイスに IP ACL と MAC ACL の両方を適用すると、同じレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックの両方をフィルタリングできます。同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。

MAC ACL がすでにレイヤ 2 インターフェイスに設定されており、新しい MAC ACL をインターフェイスに適用した場合、以前に設定されていた ACL は新しい ACL で置換されます。

スイッチ上でレイヤ 2 インターフェイスに ACL を適用する場合に、そのスイッチに対してレイヤ 3 ACL が適用されているか、またはインターフェイスがメンバである VLAN に VLAN マップが適用されていれば、レイヤ 2 インターフェイスに適用された ACL が有効になります。

スイッチは、MAC ACL が適用されたインターフェイス上で入力パケットを受信すると、その ACL 内の一致条件を調べます。条件が一致すると、スイッチは ACL に従ってパケットを転送またはドロップします。

指定された ACL が存在しない場合、スイッチはすべてのパケットを転送します。

MAC 拡張 ACL を設定する方法の詳細については、このリリース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 Network Security with ACLs」の章を参照してください。

## ■ mac access-group

## 例

次の例では、*macacl2* と名付けられた MAC 拡張 ACL をインターフェイスに適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/1  
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   |
|---------------------------------------|--|
| <a href="#">show access-lists</a>     | スイッチで設定される ACL を表示します。   |
| <a href="#">show link state group</a> | スイッチで設定される MAC ACL を表示します。   |
| <a href="#">show running-config</a>   | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、グローバル コンフィギュレーション モードで **mac access-list extended** コマンドを使用します。このコマンドを使用すると、拡張 MAC アクセス リスト コンフィギュレーション モードに入ります。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**mac access-list extended** *name*

**no mac access-list extended** *name*

## 構文の説明

*name* MAC 拡張アクセス リストに割り当てられている名前。

## コマンド デフォルト

デフォルトでは、MAC アクセス リストは作成されません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

MAC 名前付き拡張リストは、VLAN マップおよびクラス マップとともに使用されます。

名前付き MAC 拡張 ACL は、VLAN マップまたはレイヤ 2 インターフェイスに適用できます。レイヤ 3 インターフェイスには適用できません。

**mac access-list extended** コマンドを入力すると、MAC アクセス リスト コンフィギュレーション モードがイネーブルになります。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **default** : コマンドをデフォルトに設定します。
- **deny** : 拒否するパケットを指定します。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、デフォルト設定にします。
- **permit** : 転送するパケットを指定します。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。

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   |
|--|--|
| <code>deny</code> (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)。                                  |
| <code>permit</code> (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)。                                  |
| <code>show access-lists</code>                 | スイッチで設定されるアクセス リストを表示します。  |
| <code>vlan access-map</code>                   | 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

エントリが使用または更新された後、ダイナミック エントリが MAC アドレス テーブル内に保持される時間を設定するには、グローバル コンフィギュレーション モードで **mac-address-table aging-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**mac address-table aging-time** {0 | 10-1000000} [vlan vlan-id]

**no mac address-table aging-time** {0 | 10-1000000} [vlan vlan-id]

## 構文の説明

|                     |  |
|---------------------|--|
| <b>0</b>            | 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。 |
| <b>10-1000000</b>   | エージング タイム (秒)。指定できる範囲は 10 ~ 1000000 秒です。                     |
| <b>vlan vlan-id</b> | (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。     |

## コマンド デフォルト

デフォルトは 300 秒です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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。

ホストが継続してダイナミック エントリを送信しない場合、エージング タイムを長くして、より長い時間ダイナミック エントリを記録してください。時間を長くすることで、ホストが再送信した場合にフラッシングが起こりにくくなります。

特定の VLAN を指定しない場合、このコマンドはすべての VLAN に対してエージング タイムを設定します。

## 例

次の例では、すべての VLAN にエージング タイムを 200 秒に設定する方法を示します。

```
Switch(config)# mac address-table aging-time 200
```

**show mac address-table aging-time** 特権 EXEC コマンドを入力すると、設定を確認できます。

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">show mac address-table aging-time</a> | 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、グローバル コンフィギュレーション モードで **mac-address-table learning** コマンドを使用します。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

*vlan-id* 1 つの VLAN ID、またはハイフンあるいはカンマで区切った VLAN ID の範囲を指定します。指定できる VLAN ID は 1 ~ 4094 です。この VLAN を内部 VLAN にはできません。

## コマンドデフォルト

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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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 とポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。

1 つの VLAN ID (たとえば、**no mac address-table learning vlan 223**) または VLAN ID の範囲 (たとえば、**no mac address-table learning vlan 1-20, 15**) での MAC アドレス ラーニングを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、スイッチ仮想インターフェイス (SVI) 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。

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。

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
```

---

**関連コマンド**

| コマンド  | 説明   |
|---|--|
| <a href="#">show mac address-table learning</a> | 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、グローバル コンフィギュレーション モードで **mac address-table move update** コマンドを使用します。デフォルト設定に戻すには、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

|                 |   |
|-----------------|---|
| <b>receive</b>  | 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。   |
| <b>transmit</b> | 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 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 モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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実行できます。

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
```

| 関連コマンド | コマンド                                       | 説明                                  |
|--------|--|-------------------------------------|
|        | <b>clear mac address-table move update</b> | 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。 |
|        | <b>debug matm move update</b>              | 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。   |
|        | <b>show mac address-table move update</b>  | スイッチの MAC アドレス テーブル移行更新情報を表示します。    |

# mac address-table notification

スイッチ上で MAC アドレス通知機能をイネーブルにするには、グローバル コンフィギュレーション モードで **mac-address-table notification** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mac address-table notification {change [history-size value | interval value] | mac-move |
threshold [[limit percentage] interval time]}
```

```
no mac address-table notification {change [history-size value | interval value] | mac-move |
threshold [[limit percentage] interval time]}
```

## 構文の説明

|                           |   |
|---------------------------|---|
| <b>change</b>             | スイッチで MAC 通知をイネーブルまたはディセーブルにします。  |
| <b>history-size value</b> | (任意) MAC 通知履歴テーブルのエントリの最大数を設定します。指定できる範囲は 0 ~ 500 エントリです。デフォルトは 1 です。                       |
| <b>interval value</b>     | (任意) 通知トラップ間隔を設定します。この時間量が過ぎると、スイッチは通知トラップを送信します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルト値は 1 秒です。 |
| <b>mac-move</b>           | MAC 移動通知をイネーブルにします。   |
| <b>threshold</b>          | MAC しきい値通知をイネーブルにします。   |
| <b>limit percentage</b>   | (任意) MAC 利用率しきい値を入力します。指定できる範囲は 1 ~ 100% です。デフォルト値は 50% です。                                 |
| <b>interval time</b>      | (任意) MAC しきい値通知の間の時間を入力します。指定できる範囲は 120 ~ 1000000 秒です。デフォルトは 120 秒です。                       |

## コマンドデフォルト

デフォルトでは、MAC アドレス通知、MAC 移動、および MAC しきい値モニタリングがディセーブルです。

デフォルトの MAC 変更トラップ間隔は 1 秒です。

履歴テーブルのデフォルトのエントリ数は 1 です。

デフォルトの MAC 利用率しきい値は 50% です。

MAC しきい値通知間のデフォルトの時間は 120 秒です。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

MAC アドレス通知変更機能は、新しい MAC アドレスが転送テーブルに追加されたり、古いアドレスがそこから削除されたりするたびに、簡易ネットワーク管理プロトコル (SNMP) トラップをネットワーク管理システム (NMS) に送信します。MAC 変更通知はダイナミックおよびセキュア MAC アドレスだけに生成され、セルフ アドレス、マルチキャスト アドレス、または他のスタティック アドレスには生成されません。

**history-size** オプションを設定している場合、既存の MAC アドレス履歴テーブルが削除され、新しいテーブルが作成されます。

**mac address-table notification change** コマンドを使用すれば、MAC アドレス通知変更機能がイネーブルになります。また、**snmp trap mac-notification change** インターフェイス コンフィギュレーション コマンドでインターフェイス上の MAC アドレス通知トラップをイネーブルにし、**snmp-server enable traps mac-notification change** グローバル コンフィギュレーション コマンドでスイッチが MAC アドレストラップを NMS に送信するよう設定する必要があります。

また、**mac address-table notification mac-move** コマンドおよび **snmp-server enable traps mac-notification move** グローバル コンフィギュレーション コマンドを入力することにより、MAC アドレスが 1 つのポートから同じ VLAN の別のポートに移動した場合、常にトラップをイネーブルにできます。

MAC アドレス テーブルのしきい値制限に達するかそれを超えた場合に常にトラップを生成するには、**mac address-table notification threshold [limit percentage] [interval time]** コマンドおよび **snmp-server enable traps mac-notification threshold** グローバル コンフィギュレーション コマンドを入力します。

### 例

次の例では、MAC アドレス テーブル変更通知機能をイネーブルにし、通知トラップの間隔を 60 秒、履歴テーブルのサイズを 100 エントリに設定する方法を示します。

```
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 60
Switch(config)# mac address-table notification change history-size 100
```

### 関連コマンド

| コマンド  | 説明  |
|---|---|
| <b>clear mac address-table notification</b> | MAC アドレス通知グローバル カウンタをクリアします。                                  |
| <b>show mac address-table notification</b>  | 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。          |
| <b>snmp-server enable traps</b>             | <b>mac-notification</b> 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。 |
| <b>snmp trap mac-notification change</b>    | 特定のインターフェイスの SNMP MAC 通知変更トラップをイネーブルにします。                     |

# mac address-table static

スタティック アドレスを MAC アドレス テーブルに追加するには、グローバル コンフィギュレーション モードで **mac-address-table secure** 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

|                               |  |
|-------------------------------|--|
| <b>mac-addr</b>               | 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。 |
| <b>vlan vlan-id</b>           | 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。  |
| <b>interface interface-id</b> | 受信パケットが転送され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。                                     |

## コマンドデフォルト

スタティック アドレスは設定されていません。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 gigabitethernet 1/1
```

## 関連コマンド

| コマンド  | 説明                                 |
|---|------------------------------------|
| <a href="#">show mac address-table static</a> | 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、グローバル コンフィギュレーション モードで **mac address-table static drop** コマンドを使用します。デフォルト設定に戻すには、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 drop**

## 構文の説明

|                     |   |
|---------------------|---|
| <i>mac-addr</i>     | 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。                  |
| <i>vlan vlan-id</i> | 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。 |

## コマンド デフォルト

ユニキャスト MAC アドレス フィルタリングはディセーブルです。スイッチは、特定の送信元または宛先 MAC アドレスのトラフィックをドロップしません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドを使用する場合、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされません。CPU に転送されるパケットもサポートされません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、またはその MAC アドレスを持つパケットをドロップします。2 番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
```

## ■ mac address-table static 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                                 |
|---|------------------------------------|
| <a href="#">show mac address-table static</a> | 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、インターフェイス コンフィギュレーション モードで **macro apply** 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

|                        |  |
|------------------------|--|
| <b>apply</b>           | 指定したインターフェイスにマクロを適用します。  |
| <b>trace</b>           | インターフェイスにマクロを適用してマクロをデバッグします。  |
| <i>macro-name</i>      | マクロの名前。  |
| <b>parameter value</b> | (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。 |

## コマンドデフォルト

なし

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

スイッチ ソフトウェアには、シスコ デフォルト **Smartports** マクロが埋め込まれています。これらのマクロやコマンドは、**show parser macro** ユーザ EXEC コマンドを使用して表示できます。

インターフェイスにシスコ デフォルト Smartports マクロを適用する場合は、次の注意事項に従ってください。

- **show parser macro** ユーザ EXEC コマンドを使用して、スイッチ上のすべてのマクロを表示します。特定のマクロの内容を表示するには、**show parser macro name macro-name** ユーザ EXEC コマンドを使用します。
- **\$** で始まるキーワードには、一意のパラメータ値が必要です。**parameter value** キーワードを使用して、必要な値をシスコ デフォルト マクロに追加します。

シスコ デフォルト マクロは **\$** という文字を使用しているので、必須キーワードを識別するのに役立ちます。マクロを作成する場合、**\$** という文字を使用したキーワードの定義には制限がありません。

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。

**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。

## 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'
```

次の例では、シスコ デフォルト **cisco-desktop** マクロを表示する方法、およびインターフェイス上でマクロを適用し、アクセス VLAN ID を 25 に設定する方法を示します。

```
Switch# show parser macro cisco-desktop
-----
Macro name : cisco-desktop
Macro type : default

# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
```

```
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

```
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

```
-----
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

次に、インターフェイスにマクロを直接適用する例を示します。

```
Switch# configure terminal
Switch(config)#macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# macro apply duplex
```

#### 関連コマンド

| コマンド                                     | 説明                                   |
|--|--------------------------------------|
| <a href="#">macro description</a>        | 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。      |
| <a href="#">macro global</a>             | 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。 |
| <a href="#">macro global description</a> | 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。          |
| <a href="#">macro name</a>               | マクロを作成します。                           |
| <a href="#">show parser macro</a>        | 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どのマクロが適用されるかについて説明を入力するには、インターフェイス コンフィギュレーション モードで **macro description** 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 text**

## 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。

## コマンドデフォルト

なし

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 例

次に、**ab-global** の説明を含む事前定義されたグローバル マクロを使用する方法を示します。

```
Switch(config-if)# macro keywords Scip_vlan
# Macro Name ab-global
#macro global description ab-global
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
no aaa new-model
service timestamps log datetime msec localtime show-timezone
service timestamps debug datetime msec localtime show-timezone
service password-encryption
logging buffered 16384 debugging
no logging console
vtp mode transparent
udld aggressive
no ip source-route
no ip domain-lookup
ip subnet-zero
ip igmp snooping
ip igmp snooping querier
```

```
errdisable recovery cause all
errdisable recovery interval 30
spanning-tree mode mst
spanning-tree loopguard default
spanning-tree portfast bpduguard default

spanning-tree portfast bpduguard default
int vlan $cip_vlan
cip enable
exit
alarm profile ab-alarm
alarm 1 2 3 4
syslog 1 2 3 4
notifies 1 2 3 4
relay-major 2
relay-minor 1 3 4
exit
alarm facility power-supply relay major
alarm facility power-supply syslog
alarm facility power-supply notifies
alarm facility temperature primary relay major
alarm facility temperature primary syslog
alarm facility temperature primary notifies
alarm facility temperature secondary relay minor
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
alarm facility temperature secondary high 90
alarm facility temperature secondary low 0
snmp-server enable traps
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
class-map match-all CIP-Implicit_dscp_55
match access-group 101
class-map match-all CIP-Implicit_dscp_47
match access-group 102
class-map match-all CIP-Implicit_dscp_43
match access-group 103
class-map match-all CIP-Implicit_dscp_any
match access-group 104
class-map match-all CIP-Other
match access-group 105
class-map match-all 1588-PTP-Event
match access-group 106
class-map match-all 1588-PTP-General
match access-group 107
class-map match-all voip-data
match ip dscp ef
class-map match-all voip-control
match ip dscp cs3 af31
policy-map Voice-Map
class voip-data
set dscp ef
police 320000 8000 exceed-action policed-dscp-transmit
class voip-control
set dscp cs3
police 32000 8000 exceed-action policed-dscp-transmit
policy-map CIP-PTP-Traffic
class CIP-Implicit_dscp_55
```

## macro description

```

set ip dscp 55
class CIP-Implicit_dscp_47
set ip dscp 47
class CIP-Implicit_dscp_43
set ip dscp 43
class CIP-Implicit_dscp_any
set ip dscp 31
class CIP-Other
set ip dscp 27
class 1588-PTP-Event
set ip dscp 59
class 1588-PTP-General
set ip dscp 47
Switch(config-if)#

```

## 関連コマンド

| コマンド                                     | 説明   |
|--|--|
| <a href="#">macro apply</a>              | 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。 |
| <a href="#">macro global</a>             | 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。         |
| <a href="#">macro global description</a> | 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。                  |
| <a href="#">macro name</a>               | マクロを作成します。                                   |
| <a href="#">show parser macro</a>        | 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

定義済みマクロの説明を使用するには、グローバル インターフェイス モードで **macro description** コマンドを使用します。

## macro description *line*

|            |                             |                 |
|------------|-----------------------------|-----------------|
| 構文の説明      | <i>line</i>                 | グローバル マクロの名前。   |
| コマンド デフォルト | なし                          |                 |
| コマンド モード   | グローバル インターフェイス コンフィギュレーション。 |                 |
| コマンド履歴     | リリース                        | 変更内容            |
|            | 15.0(1)EY                   | このコマンドが導入されました。 |

**使用上のガイドライン** Smartport マクロは、事前設定を使用することにより、スイッチの設定を簡素化します。QoS の機能拡張、スパニングツリー、セキュリティなどの CLI の設定を学習する代わりに、接続されたデバイス タイプに基づいてポートを示し、クリックすることで設定できます。すべての設定およびテストは、Rockwell および Cisco Systems が出荷前にすでに行っています。

**例** 次に、**ab-global** の説明を含む事前定義されたグローバル マクロを使用する方法を示します。

```
Switch(config-if)# macro keywords $cip_vlan
# Macro Name ab-global
#macro global description ab-global

service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
no aaa new-model
service timestamps log datetime msec localtime show-timezone
service timestamps debug datetime msec localtime show-timezone
service password-encryption
logging buffered 16384 debugging
no logging console
vtp mode transparent
udld aggressive
no ip source-route
no ip domain-lookup
ip subnet-zero
ip igmp snooping
ip igmp snooping querier
errdisable recovery cause all
errdisable recovery interval 30
spanning-tree mode mst
spanning-tree loopguard default
spanning-tree portfast bpduguard default
spanning-tree portfast bpdufilter default
```

```

int vlan $cip_vlan
  cip enable
exit
alarm profile ab-alarm
alarm 1 2 3 4
syslog 1 2 3 4
notifies 1 2 3 4
relay-major 2
relay-minor 1 3 4
exit
alarm facility power-supply relay major
alarm facility power-supply syslog
alarm facility power-supply notifies
alarm facility temperature primary relay major
alarm facility temperature primary syslog
alarm facility temperature primary notifies
alarm facility temperature secondary relay minor
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
alarm facility temperature secondary high 90
alarm facility temperature secondary low 0
snmp-server enable traps
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
class-map match-all CIP-Implicit_dscp_55
  match access-group 101
class-map match-all CIP-Implicit_dscp_47
  match access-group 102
class-map match-all CIP-Implicit_dscp_43
  match access-group 103
class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Other
  match access-group 105
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all 1588-PTP-General
  match access-group 107
class-map match-all voip-data
  match ip dscp ef
class-map match-all voip-control
  match ip dscp cs3 af31
policy-map Voice-Map
  class voip-data
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class voip-control
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
policy-map CIP-PTP-Traffic
  class CIP-Implicit_dscp_55
    set ip dscp 55
  class CIP-Implicit_dscp_47
    set ip dscp 47
  class CIP-Implicit_dscp_43
    set ip dscp 43
  class CIP-Implicit_dscp_any
    set ip dscp 31

```

```
class CIP-Other
  set ip dscp 27
class 1588-PTP-Event
  set ip dscp 59
class 1588-PTP-General
  set ip dscp 47
Switch(config-if)#
```

---

**関連コマンド**

| コマンド                            | 説明                |
|---------------------------------|-------------------|
| <b>macro global description</b> | 定義済みマクロの説明を使用します。 |

---

# macro global

スイッチにマクロを適用するか、またはスイッチ上でマクロを適用および追跡するには、グローバル コンフィギュレーション モードで **macro global** 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

|                        |  |
|------------------------|--|
| <b>apply</b>           | スイッチにマクロを適用します。  |
| <b>trace</b>           | 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>      | マクロの名前。  |
| <b>parameter value</b> | (任意) そのスイッチに限定された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。 |

## コマンドデフォルト

なし

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

スイッチ ソフトウェアには、シスコ デフォルト **Smartports** マクロが埋め込まれています。これらのマクロやコマンドは、**show parser macro** ユーザ EXEC コマンドを使用して表示できます。

スイッチにシスコ デフォルト Smartports マクロを適用するときは、次の注意事項に従ってください。

- **show parser macro** ユーザ EXEC コマンドを使用して、スイッチ上のすべてのマクロを表示します。特定のマクロの内容を表示するには、**show parser macro name macro-name** ユーザ EXEC コマンドを使用します。
- **\$** で始まるキーワードには、一意のパラメータ値が必要です。 **parameter value** キーワードを使用して、必要な値をシスコ デフォルト マクロに追加します。

シスコ デフォルト マクロは **\$** という文字を使用しているため、必須キーワードを識別するのに役立ちます。マクロを作成する場合、**\$** という文字を使用したキーワードの定義には制限がありません。

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。

マクロに含まれる各コマンドの **no** バージョンを入力したときにだけ、スイッチで適用されたグローバル マクロ設定を削除できます。

## 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、**addresss** 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'
```

次の例では、マクロを直接グローバルに適用する方法を示します。

```
Switch# configure terminal
Switch(config)# macro global apply test-macro
Switch(config)#
```

## 関連コマンド

| コマンド                                     | 説明   |
|--|--|
| <a href="#">macro apply</a>              | 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。 |
| <a href="#">macro description</a>        | 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。              |
| <a href="#">macro global description</a> | 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。                  |
| <a href="#">macro name</a>               | マクロを作成します。                                   |
| <a href="#">show parser macro</a>        | 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、グローバル コンフィギュレーション モードで **macro global description** 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** *text*

## 構文の説明

*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。

## コマンドデフォルト

なし

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 uddld 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   |
|-----------------------------------|--|
| <a href="#">macro apply</a>       | 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。 |
| <a href="#">macro description</a> | 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。              |
| <a href="#">macro global</a>      | 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。         |
| <a href="#">macro name</a>        | マクロを作成します。                                   |
| <a href="#">show parser macro</a> | 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、グローバル コンフィギュレーション モードで **macro name** 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

### コマンドデフォルト

なし

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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。または、元のマクロの対応するすべてのコマンドの **no** 形式を含む既存のマクロに対して、アンチマクロを作成し、インターフェイスにそのアンチマクロを適用できます。

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 gigabitethernet 1/1
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   |
|--|--|
| <a href="#">macro apply</a>              | 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。 |
| <a href="#">macro description</a>        | 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。              |
| <a href="#">macro global</a>             | 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。         |
| <a href="#">macro global description</a> | 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。                  |
| <a href="#">show parser macro</a>        | 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 1 つまたは複数のアクセス リストとパケットとを照合するように設定するには、アクセスマップ モードで **match access-map** 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

|                    |  |
|--------------------|--|
| <b>ip address</b>  | 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。          |
| <b>mac address</b> | 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。 |

## コマンド デフォルト

デフォルトのアクションでは、一致パラメータは VLAN マップに適用されません。

## コマンド モード

アクセス マップ コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 a12 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 a12
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   |
|---------------------------------|--|
| <b>access-list</b>              | 番号付き標準 ACL を設定します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。  |
| <b>ip access-list</b>           | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>mac access-list extended</b> | 名前付き MAC アドレス アクセス リストを作成します。  |
| <b>show access-lists</b>        | パケットがアクセス コントロール リスト (ACL) のエントリに一致した場合に、実行されるアクションを指定します。   |
| <b>show vlan access-map</b>     | スイッチで作成された VLAN アクセス マップを表示します。  |
| <b>vlan access-map</b>          | VLAN アクセス マップを作成します。   |

## match (クラスマップコンフィギュレーション)

トラフィックを分類するための一致基準を定義するには、クラスマップコンフィギュレーションモードで **match** コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

```
match {access-group acl-index-or-name | input-interface interface-id-list | ip dscp dscp-list | ip precedence ip-precedence-list}
```

```
no match {access-group acl-index-or-name | input-interface interface-id-list | ip dscp dscp-list | ip precedence ip-precedence-list}
```

### 構文の説明

|  |  |
|--|--|
| <b>access-group</b><br><i>acl-index-or-name</i>    | IP 標準または拡張アクセスコントロールリスト (ACL) または MAC ACL の番号または名前を指定します。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。   |
| <b>input-interface</b><br><i>interface-id-list</i> | 階層ポリシー マップでインターフェイス レベルのクラス マップを適用する物理ポートを指定します。このコマンドは、子レベルのポリシー マップでだけ使用でき、子レベルのポリシー マップ内での唯一の一致条件である必要があります。ポート (1 エントリとしてカウント)、スペースで区切ったポート (各ポートを 1 エントリとしてカウント)、またはハイフンで区切ったポート範囲 (2 エントリとしてカウント) を指定することによって、最大 6 つのエントリを指定することができます。<br><br>このオプションは、スイッチが IP サービス イメージを稼働している場合にのみ使用できます。 |
| <b>ip dscp</b> <i>dscp-list</i>                    | 着信パケットとの照合を行うための IP DiffServ コードポイント (DSCP) 値を最大 8 つまで列挙します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。よく使用される値の場合は、ニーモニック名を入力することもできます。   |
| <b>ip precedence</b><br><i>ip-precedence-list</i>  | 着信パケットとの照合を行うための、IP precedence 値を最大 8 つまで列挙します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。よく使用される値の場合は、ニーモニック名を入力することもできます。   |

### コマンド デフォルト

一致基準は定義されません。

### コマンド モード

クラスマップコンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

パケットを分類するために着信パケットのどのフィールドを調べるのかを指定する場合は、**match** コマンドを使用します。IP アクセス グループまたは MAC アクセス グループの Ether Type/Len のマッチングだけがサポートされています。

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

**match ip dscp dscp-list** コマンドまたは **match ip precedence ip-precedence-list** コマンドの場合は、よく使用される値のニーモニック名を入力できます。たとえば、**match ip dscp af11** コマンドを入力できます。このコマンドは、**match ip dscp 10** コマンドを入力した場合と同じ結果になります。また、**match ip precedence critical** コマンドを入力できます。このコマンドは、**match ip precedence 5** コマンドを入力した場合と同じ結果になります。サポートされているニーモニックのリストを表示するには、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドラインのヘルプストリングを表示してください。

階層ポリシー マップ内にインターフェイス レベルのクラス マップを設定するときには、**input-interface interface-id-list** キーワードを使用します。*interface-id-list* には、最大 6 つのエントリを指定することができます。

## 例

次の例では、クラス マップ **class2** を作成する方法を示します。このマップは、DSCP 値 10、11、および 12 を持つすべての着信トラフィックに一致します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

次の例では、クラス マップ **class3** を作成する方法を示します。このマップは、IP precedence 値 5、6、および 7 を持つすべての着信トラフィックに一致します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

次の例では、IP precedence 一致基準を削除し、**acl1** を使用してトラフィックを分類する方法を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートのリストの指定方法を示しています。

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet1/1 gigabitethernet1/2
Switch(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートの範囲の指定方法を示しています。

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet1/1 - gigabitethernet1/5
Switch(config-cmap)# exit
```

## 関連コマンド

| コマンド                  | 説明                                      |
|-----------------------|---|
| <b>class-map</b>      | 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。 |
| <b>show class-map</b> | 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、インターフェイス コンフィギュレーション モードで **mdix auto** コマンドを使用します。システムの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。

**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。

## コマンドデフォルト

Auto MDIX は、イネーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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。

インターフェイスの Auto MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイス速度とデュプレックスも **auto** に設定する必要があります。

Auto MDIX が（速度とデュプレックスの自動ネゴシエーションとともに）接続するインターフェイスの一方または両方でイネーブルの場合は、ケーブルタイプ（ストレートまたはクロス）が不正でもリンクがアップします。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mbps インターフェイス上および 10/100/1000BASE-T/TX Small Form-Factor Pluggable (SFP) モジュール インターフェイス上でサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

## 例

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

# media-type rj45

USB および RS-232 ケーブルの両方が接続されている場合、USB 接続の優先順位を変更するには、グローバルなライン コンソール コンフィギュレーション モードで **media-type rj45** コマンドを使用します。

```
media-type rj45
```

```
no media-type rj45
```

**コマンド デフォルト** RS-232 ケーブルが接続に使用されます。

**コマンド モード** グローバルなライン コンソール コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン** R-J45 と RS-232 ケーブルの両方がある場合は、**media-type rj45** コマンドを使用して USB 接続から RJ-45 接続にケーブル接続を変更できます。

**例** 次に、RJ-45 ケーブル接続に切り替える例を示します。

```
Switch(config)# line console 0
Switch(config-line)# media-type rj45
Switch(config-line)#
```

## 関連コマンド

| コマンド   | 説明                                      |
|--|---|
| <a href="#">show interfaces capabilities</a>           | 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。    |
| <a href="#">show interfaces transceiver properties</a> | インターフェイスの速度とデュプレックスの設定およびメディアタイプを表示します。 |

# mls qos

スイッチ全体の Quality of Service (QoS) をイネーブルにするには、グローバル コンフィギュレーション モードで **mls qos** コマンドを使用します。スイッチ全体のすべての QoS 関連の統計をリセットし、QoS 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**mls qos**

**no mls qos**



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 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 デフォルト

QoS はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**mls qos** コマンドを入力すると、システム内のすべてのポートでデフォルト パラメータが使用されて QoS がイネーブルになります。

パケットが変更されない (パケット内の CoS、DSCP、および IP precedence 値は変更されない) ため、信頼できるポートまたは信頼できないポートといった概念は存在しません。トラフィックは Pass-Through モードでスイッチングされます (パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます)。

**mls qos** グローバル コンフィギュレーション コマンドによって QoS がイネーブル化され、その他のすべての QoS 設定値がデフォルト値に設定されている場合、トラフィックはポリシングされず、ベスト エフォート (DSCP 値と CoS 値は 0 に設定される) として分類されます。ポリシー マップは設定されません。すべてのポート上のデフォルト ポートの信頼性は、信頼性なし (untrusted) の状態です。デフォルトの入力キューおよび出力キューの設定値が有効となります。

QoS 分類、ポリシング、マークダウンまたはドロップ、キューイング、トラフィック シェーピング機能を使用するには、QoS をグローバルにイネーブルにする必要があります。**mls qos** コマンドを入力する前に、ポリシー マップを作成し、それをポートに適用できます。ただし、**mls qos** コマンドを入力していない場合、QoS 処理はディセーブルになります。

**no mls qos** コマンドを入力しても、QoS を設定するために使用したポリシー マップとクラス マップは設定から削除されません。ただし、システム リソースを節約するため、ポリシー マップに対応するエントリはスイッチ ハードウェアから削除されます。以前の設定で QoS を再度イネーブルにするには、**mls qos** コマンドを使用します。

このコマンドでスイッチの QoS 状態を切り替えることで、キューのサイズが修正 (再割り当て) されます。キュー サイズの変更時には、ハードウェアを再設定する期間中キューは一時的にシャットダウンされ、スイッチはこのキューに新たに到着したパケットをドロップします。

**例**

次の例では、スイッチ上で QoS をイネーブルにする方法を示します。

```
Switch(config)# mls qos
```

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

**関連コマンド**

| コマンド                         | 説明            |
|------------------------------|---------------|
| <a href="#">show mls qos</a> | QoS 情報を表示します。 |

# mls qos aggregate-policer

同じポリシー マップ内の複数のクラスが共有できるポリサー パラメータを定義するには、グローバル コンフィギュレーション モードで **mls qos aggregate-policer** コマンドを使用します。集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

```
mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte exceed-action {drop |
  policed-dscp-transmit}
```

```
no mls qos aggregate-policer aggregate-policer-name
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |  |
|--|--|
| <i>aggregate-policer-name</i>              | <b>police aggregate</b> ポリシー マップ クラス コンフィギュレーション コマンドが参照する集約ポリサーの名前です。                             |
| <i>rate-bps</i>                            | ビット/秒 (b/s) の平均トラフィック伝送速度。指定できる範囲は 8000 ~ 1000000000 です。   |
| <i>burst-byte</i>                          | 通常のバースト サイズ (バイト単位)。指定できる範囲は 8000 ~ 1000000 です。  |
| <b>exceed-action drop</b>                  | 指定された伝送速度を超えたときにスイッチがパケットをドロップするよう指定します。   |
| <b>exceed-action policed-dscp-transmit</b> | 指定された伝送速度を超えると、スイッチがパケットの Diffserv コード ポイント (DSCP) をポリシング設定 DSCP マップに指定された値に変更して、パケットを送信するよう指定します。 |

## コマンド デフォルト

集約ポリサーは定義されません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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。

ポリサーが複数のクラスによって共有されている場合は、集約ポリサーを定義します。

あるポートのポリサーを別のポートの他のポリサーと共有することはできません。2 つの異なるポートからのトラフィックは、ポリシング目的では集約できません。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー (255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー) をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません (ポートがいずれかのポリサーに割り当てられるとは保証されていません)。

集約ポリサーは同じポリシー マップ内の複数のクラスに適用されます。異なるポリシー マップにまたがって集約ポリサーを使用することはできません。

ポリシー マップ内で使用中の場合、集約ポリサーは削除できません。最初に、**no police aggregate aggregate-policer-name** ポリシー マップ クラス コンフィギュレーション コマンドを使用してすべてのポリシー マップから集約ポリサーを削除してから、**no mls qos aggregate-policer aggregate-policer-name** コマンドを使用する必要があります。

ポリシングは、トークンバケットアルゴリズムを使用します。バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。トークンがバケットから削除される速度（平均速度）を設定するには、*police* ポリシー マップ クラス コンフィギュレーション コマンドの **rate-bps** オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

## 例

次の例では、集約ポリサー パラメータを定義する方法と、ポリシー マップ内の複数のクラスにそのポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

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

## 関連コマンド

| コマンド                                  | 説明                                       |
|---------------------------------------|--|
| <b>police aggregate</b>               | 異なるクラスによって共有されるポリサーを作成します。               |
| <b>show mls qos aggregate-policer</b> | Quality of Service (QoS) 集約ポリサー設定を表示します。 |

# mls qos cos

デフォルトのポート サービスクラス (CoS) 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てるには、インターフェイス コンフィギュレーション モードで **mls qos cos** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos cos {default-cos | override}
```

```
no mls qos cos {default-cos | override}
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                    |   |
|--------------------|---|
| <i>default-cos</i> | デフォルトのポート CoS 値。パケットがタグ付けされていない場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ~ 7 です。 |
| <b>override</b>    | 着信パケットの CoS を上書きし、ポートのデフォルト CoS 値をすべての着信パケットに適用します。                                     |

## コマンド デフォルト

デフォルトのポート CoS 値は 0 です。  
CoS 無効化はディセーブルに設定されています。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

デフォルト値を使用して、タグなし (着信パケットが CoS 値を持たない場合) で着信したすべてのパケットに CoS 値と Diffserv コード ポイント (DSCP) 値を割り当てることができます。また、**override** キーワードを使用すると、デフォルトの CoS 値と DSCP 値をすべての着信パケットに割り当てることができます。

特定のポートに届くすべての着信パケットに、他のポートから着信するパケットより高いプライオリティまたは低いプライオリティを与える場合には、**override** キーワードを使用します。たとえポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されていても、このコマンドは以前に設定済みの信頼状態を無効にし、すべての着信 CoS 値に **mls qos cos** コマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、パケットの CoS 値は、出力ポートで、ポートのデフォルト CoS を使用して変更されます。

**例**

次の例では、ポートのデフォルト ポート CoS 値を 4 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

次の例では、ポートで、ポートに着信するすべてのパケットにデフォルトのポート CoS 値 4 を割り当てる方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

**show mls qos interface** 特権 EXEC コマンドを入力すると、設定を確認できます。

**関連コマンド**

| コマンド                                   | 説明                                 |
|--|------------------------------------|
| <a href="#">show mls qos interface</a> | Quality of Service (QoS) 情報を表示します。 |

# mls qos dscp-mutation

Diffserv コードポイント (DSCP) /DSCP 変換マップを DSCP の信頼性のあるポートに適用するには、インターフェイス コンフィギュレーション モードで **mls qos dscp-mutation** コマンドを使用します。マップをデフォルト設定 (DSCP 変換なし) に戻すには、このコマンドの **no** 形式を使用します。

**mls qos dscp-mutation** *dscp-mutation-name*

**no mls qos dscp-mutation** *dscp-mutation-name*



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                           |  |
|---------------------------|--|
| <i>dscp-mutation-name</i> | DSCP/DSCP 変換マップの名前。このマップは、以前は <b>mls qos map dscp-mutation</b> グローバル コンフィギュレーション コマンドで定義されていました。 |
|---------------------------|--|

## コマンド デフォルト

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

2 つの Quality of Service (QoS) ドメインが異なる DSCP 定義を持つ場合は、DSCP/DSCP 変換マップを使用して、一方の DSCP 値のセットをもう一方のドメインの定義に適合するように変換します。DSCP/DSCP 変換マップは、Quality of Service (QoS) 管理ドメインの境界にある受信ポートに適用します (入力変換)。

入力変換では、新しい DSCP 値がパケット内の値を上書きし、QoS はこの新しい値を持つパケットを処理します。スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

入力ポートには複数の DSCP/DSCP 変換マップを設定できます。

マップは、DSCP の信頼性のあるポートにだけ適用します。DSCP 変換マップを信頼できないポート、Class of Service (CoS) または IP precedence の信頼できるポートに適用すると、コマンドはすぐには影響せず、そのポートが DSCP の信頼できるポートになってから効果を発揮します。

## 例

次の例では、DSCP/DSCP 変換マップ `dscpmutation1` を定義し、そのマップをポートに適用する方法を示します。

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

次の例では、DSCP/DSCP 変換マップ名 `dscpmutation1` をポートから削除し、そのマップをデフォルトにリセットする方法を示します。

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

設定を確認するには、`show mls qos maps` 特権 EXEC コマンドを入力します。

#### 関連コマンド

| コマンド                                   | 説明                     |
|--|------------------------|
| <code>mls qos map dsep-mutation</code> | DSCP/DSCP 変換マップを定義します。 |
| <code>mls qos trust</code>             | ポートの信頼状態を設定します。        |
| <code>show mls qos maps</code>         | QoS のマッピング情報を表示します。    |

# mls qos map

サービスクラス (CoS) /DiffServ コードポイント (DSCP) マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシング設定 DSCP マップを定義するには、グローバル コンフィギュレーション モードで **mls qos map** コマンドを使用します。デフォルトのマップに戻すには、このコマンドの **no** 形式を使用します。

```
mls qos map {cos-dscp dscp1...dscp8 | dscp-cos dscp-list to cos | dscp-mutation
dscp-mutation-name in-dscp to out-dscp | ip-prec-dscp dscp1...dscp8 | policed-dscp dscp-list
to mark-down-dscp}
```

```
no mls qos map {cos-dscp | dscp-cos | dscp-mutation dscp-mutation-name | ip-prec-dscp |
policed-dscp}
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|   |  |
|---|--|
| <b>cos-dscp</b> <i>dscp1...dscp8</i>                                  | CoS/DSCP マップを定義します。<br><br><i>dscp1...dscp8</i> には、CoS 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。   |
| <b>dscp-cos</b> <i>dscp-list to cos</i>                               | DSCP/CoS マップを定義します。<br><br><i>dscp-list</i> には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。さらに、 <b>to</b> キーワードを入力します。<br><br><i>cos</i> には、DSCP 値と対応する 1 つの CoS 値を入力します。指定できる範囲は 0 ~ 7 です。                                    |
| <b>dscp-mutation</b><br><i>dscp-mutation-name in-dscp to out-dscp</i> | DSCP/DSCP 変換マップを定義します。<br><br><i>dscp-mutation-name</i> には、変換マップ名を入力します。<br><br><i>in-dscp</i> には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。さらに、 <b>to</b> キーワードを入力します。<br><br><i>out-dscp</i> には、1 つの DSCP 値を入力します。<br><br>指定できる範囲は 0 ~ 63 です。 |
| <b>ip-prec-dscp</b><br><i>dscp1...dscp8</i>                           | IP-precedence-to-DSCP マップを定義します。<br><br><i>dscp1...dscp8</i> には、IP precedence 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。  |
| <b>policed-dscp</b> <i>dscp-list to mark-down-dscp</i>                | ポリシング設定 DSCP マップを定義します。<br><br><i>dscp-list</i> には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。さらに、 <b>to</b> キーワードを入力します。<br><br><i>mark-down-dscp</i> には、対応するポリシング設定 (マークダウンされた) DSCP 値を入力します。<br><br>指定できる範囲は 0 ~ 63 です。                       |

## コマンド デフォルト

表 2-7 に、デフォルトの CoS/DSCP マップを示します。

表 2-7 デフォルトの CoS/DSCP マップ

| CoS 値 | DSCP 値 |
|-------|--------|
| 0     | 0      |
| 1     | 8      |
| 2     | 16     |
| 3     | 24     |
| 4     | 32     |
| 5     | 40     |
| 6     | 48     |
| 7     | 56     |

表 2-8 に、デフォルトの DSCP/CoS マップを示します。

表 2-8 デフォルトの DSCP/CoS マップ

| DSCP 値  | CoS 値 |
|---------|-------|
| 0 ~ 7   | 0     |
| 8 ~ 15  | 1     |
| 16 ~ 23 | 2     |
| 24 ~ 31 | 3     |
| 32 ~ 39 | 4     |
| 40 ~ 47 | 5     |
| 48 ~ 55 | 6     |
| 56 ~ 63 | 7     |

表 2-9 に、デフォルトの IP precedence/DSCP マップを示します。

表 2-9 デフォルトの IP Precedence/DSCP マップ

| IP precedence 値 | DSCP 値 |
|-----------------|--------|
| 0               | 0      |
| 1               | 8      |
| 2               | 16     |
| 3               | 24     |
| 4               | 32     |
| 5               | 40     |
| 6               | 48     |
| 7               | 56     |

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

**コマンドモード**

グローバル コンフィギュレーション

**コマンド履歴**

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン**

マップはすべてグローバルに定義されています。DSCP/DSCP 変換マップを除くすべてのマップは、すべてのポートに適用されます。DSCP/DSCP 変換マップは、特定のポートに適用されます。

**例**

次の例では、IP precedence/DSCP マップを定義し、IP precedence 値 0～7 を DSCP 値 0、10、20、30、40、50、55、および 60 にマッピングする方法を示します。

```
Switch# configure terminal
Switch(config)# mls qos map ip-prec-dscp 0 10 20 30 40 50 55 60
```

次の例では、ポリシング設定 DSCP マップを定義する方法を示します。DSCP 値 1、2、3、4、5、および 6 は DSCP 値 0 にマークダウンされます。明示的に設定されていないマークされた DSCP 値は変更されません。

```
Switch# configure terminal
Switch(config)# mls qos map policed-dscp 1 2 3 4 5 6 to 0
```

次の例では、DSCP/CoS マップを定義する方法を示します。DSCP 値 20、21、22、23、および 24 は、CoS 1 にマッピングされます。DSCP 値 10、11、12、13、14、15、16、および 17 は CoS 0 にマッピングされます。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 20 21 22 23 24 to 1
Switch(config)# mls qos map dscp-cos 10 11 12 13 14 15 16 17 to 0
```

次の例では、CoS/DSCP マップを定義する方法を示します。CoS 値 0～7 は、DSCP 値 0、5、10、15、20、25、30、および 35 にマッピングされます。

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 0 5 10 15 20 25 30 35
```

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。明示的に設定されていないエントリはすべて変更されません（ヌルマップ内の指定のままです）。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

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

## 関連コマンド

| コマンド                                  | 説明                                      |
|---------------------------------------|---|
| <a href="#">mls qos dscp-mutation</a> | DSCP/DSCP 変換マップを DSCP の信頼性のあるポートに適用します。 |
| <a href="#">show mls qos maps</a>     | Quality of Service (QoS) マッピング情報を表示します。 |

# mls qos queue-set output buffers

バッファをキューセットに割り当てるには（ポートあたり 4 つの出力キュー）、グローバル コンフィギュレーション モードで **mls qos queue-set output buffers** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**mls qos queue-set output *qset-id* buffers *allocation1* ... *allocation4***

**no mls qos queue-set output *qset-id* buffers**



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <i>qset-id</i>                               | キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ~ 2 です。   |
| <i>allocation1</i> ...<br><i>allocation4</i> | 各キュー（キュー 1 ~ 4 の 4 つのキュー）のバッファスペース割り当て（%）です。 <i>allocation1</i> 、 <i>allocation3</i> 、 <i>allocation4</i> の場合、範囲は 0 ~ 99 です。 <i>allocation2</i> の場合、範囲は 1 ~ 100 です（CPU バッファを含める）。各値はスペースで区切ります。 |

## コマンドデフォルト

すべての割り当て値は、4 つのキューに均等にマッピングされます（25、25、25、25）。各キューがバッファスペースの 1/4 を持ちます。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

4 つの割り当て値を指定します。各値はスペースで区切ります。

トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。

異なる特性を持つ異なるクラスのトラフィックを設定するには、**mls qos queue-set output *qset-id* threshold** グローバル コンフィギュレーション コマンドとともに、このコマンドを使用します。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

## 例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。出力キュー 1 にバッファ スペースの 40% を、出力キュー 2、3、および 4 にはそれぞれ 20% ずつ割り当てます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                      | 説明   |
|---|--|
| <b>mls qos queue-set output threshold</b> | 重み付けテーブル ドロップ (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当てを設定します。 |
| <b>queue-set</b>                          | ポートをキューセットにマッピングします。   |
| <b>show mls qos interface buffers</b>     | Quality of Service (QoS) 情報を表示します。                                   |
| <b>show mls qos queue-set</b>             | キューセットの出力キューセット値を表示します。  |

# mls qos queue-set output threshold

重み付けテールドロップ (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当て (ポートあたり 4 つの出力キュー) 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 **mls qos queue-set output threshold** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2
reserved-threshold maximum-threshold
```

```
no mls qos queue-set output qset-id threshold [queue-id]
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <i>qset-id</i>                                   | キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ~ 2 です。               |
| <i>queue-id</i>                                  | コマンドが実行されるキューセット内の特定のキューです。指定できる範囲は 1 ~ 4 です。   |
| <i>drop-threshold1</i><br><i>drop-threshold2</i> | キューに割り当てられたメモリの割合 (%) で表される 2 つの WTD しきい値です。指定できる範囲は 1 ~ 3200% です。                        |
| <i>reserved-threshold</i>                        | キューに対して保証 (予約) されるメモリ量です。割り当てられたメモリの割合 (%) で表されます。指定できる範囲は 1 ~ 100% です。                   |
| <i>maximum-threshold</i>                         | フル状態のキューが、予約量を超えるバッファを取得できるようにします。これは、キューがパケットをドロップせずに保持できる最大メモリです。指定できる範囲は 1 ~ 3200% です。 |

## コマンド デフォルト

Quality of Service (QoS) がイネーブルなときは、WTD もイネーブルです。

表 2-10 は、デフォルトの WTD しきい値の設定値を示しています。

表 2-10 デフォルトの出力キュー WTD しきい値設定値

| 機能             | キュー 1 | キュー 2 | キュー 3 | キュー 4 |
|----------------|-------|-------|-------|-------|
| WTD ドロップしきい値 1 | 100%  | 200%  | 100%  | 100%  |
| WTD ドロップしきい値 2 | 100%  | 200%  | 100%  | 100%  |
| 予約済みしきい値       | 50%   | 100%  | 50%   | 50%   |
| 最大しきい値         | 400%  | 400%  | 400%  | 400%  |

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**mls qos queue-set output *qset-id* buffers** グローバル コンフィギュレーション コマンドは、キューセット内の4つのキューに固定数のバッファを割り当てます。

ドロップしきい値 (%) は 100% を超過することができ、最大値まで指定することができます (最大しきい値が 100% を超える場合)。

バッファ範囲により、キューセット内の個々のキューが共通のプールをさらに利用できる場合でも、各キューの最大パケット数は内部で 400%、つまりバッファに割り当てられた数の4倍に制限されます。1つのパケットは1つまたは複数のバッファを使用できます。

Cisco IOS Release 15.0(25)SEE1 以降で、*drop-threshold*、*drop-threshold2*、*maximum-threshold* パラメータの範囲が増加しました。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

スイッチは、バッファ割り当て方式を使用して、出力キューごとに最小バッファ量を予約し、いずれかのキューまたはポートがすべてのバッファを消費しその他のキューがバッファを使用できなくなるのを防ぎ、バッファ スペースを要求元のキューに許可するかどうかを決定します。スイッチは、ターゲットキューが予約量を超えるバッファを消費していないかどうか (アンダーリミット)、その最大バッファをすべて消費したかどうか (オーバーリミット)、共通のプールが空 (空きバッファがない) か空でない (空きバッファ) かを判断します。キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール (空でない場合) からバッファ スペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

## 例

次の例では、ポートをキューセット2にマッピングする方法を示します。キュー2のドロップしきい値を割り当てられたメモリの40%と60%に設定し、割り当てられたメモリの100%を保証 (予約) して、このキューがパケットをドロップせずに保持可能な最大メモリを200%に設定します。

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface [*interface-id*] buffers** または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                    | 説明                      |
|---|-------------------------|
| <b>mls qos queue-set output buffers</b> | バッファをキューセットに割り当てます。     |
| <b>queue-set</b>                        | ポートをキューセットにマッピングします。    |
| <b>show mls qos interface buffers</b>   | QoS 情報を表示します。           |
| <b>show mls qos queue-set</b>           | キューセットの出力キューセット値を表示します。 |

# mls qos rewrite ip dscp

着信 IP パケットの DiffServ コードポイント (DSCP) フィールドを変更するようにスイッチを設定するには、グローバル コンフィギュレーション モードで **mls qos rewrite ip dscp** コマンドを使用します。スイッチがパケットの DSCP フィールドを変更 (書き換え) しないように設定し、DSCP 透過をイネーブルにするには、このコマンドの **no** 形式を使用します。

**mls qos rewrite ip dscp**

**no mls qos rewrite ip dscp**



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 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 デフォルト

DSCP 透過はディセーブルです。スイッチは着信 IP パケットの DSCP フィールドを変更します。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

DSCP 透過は、出力でのパケットの DSCP フィールドにだけ影響を与えます。 **no mls qos rewrite ip dscp** コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

デフォルトでは、DSCP 透過性はディセーブルです。スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて Quality of Service (QoS) に基づきます。

DSCP 透過の設定に関係なく、スイッチは、トラフィックのプライオリティを表す Class of Service (CoS) 値の生成に使用するパケットの内部 DSCP 値を変更します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

たとえば、QoS がイネーブルになっていて、着信パケットの DSCP 値が 32 である場合、スイッチは、ポリシー マップ設定に基づいて内部 DSCP 値を 16 に変更します。DSCP 透過がイネーブルになっている場合、送信 DSCP 値は 32 (着信の値と同じ) です。DSCP 透過がディセーブルになっている場合、内部 DSCP 値に基づいて、送信 DSCP 値は 16 になります。

## 例

次の例では、DSCP 透過性をイネーブルにして、スイッチで着信 IP パケットの DSCP 値を変更しないように設定する方法を示しています。

```
Switch(config)# mls qos  
Switch(config)# no mls qos rewrite ip dscp
```

次の例では、DSCP 透過性をディセーブルにして、スイッチで着信 IP パケットの DSCP 値を変更するように設定する方法を示しています。

```
Switch(config)# mls qos  
Switch(config)# mls qos rewrite ip dscp
```

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

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">mls qos</a>                               | QoS をグローバルにイネーブルにします。  |
| <a href="#">show mls qos</a>                          | QoS 情報を表示します。  |
| <a href="#">show running-config   include rewrite</a> | DSCP 透過性設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# mls qos srr-queue input bandwidth

シェイプド ラウンドロビン (SRR) の重みを入力キューに割り当てるには、グローバル コンフィギュレーション モードで **mls qos srr-queue input bandwidth** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**mls qos srr-queue input bandwidth weight1 weight2**

**no mls qos srr-queue input bandwidth**



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

*weight1 weight2* *weight1* および *weight2* の比率により、SRR スケジューラがパケットを入力キュー 1 およびキュー 2 から送り出す頻度の比率が決まります。指定できる範囲は 1 ~ 100 です。各値はスペースで区切ります。

## コマンド デフォルト

*weight1* と *weight2* は 4 です (帯域幅の 1/2 ずつ 2 つのキューに均等に分配されます)。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。

SRR は、**mls qos srr-queue input priority-queue queue-id bandwidth weight** グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth weight1 weight2** グローバル コンフィギュレーション コマンドで設定された重みで指定した通りにサービスを行います。

どの入力キューがプライオリティ キューであるかを指定するには、**mls qos srr-queue input priority-queue** グローバル コンフィギュレーション コマンドを使用します。

## 例

次の例では、キューの入力帯域幅を割り当てる方法を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/ (25+75)、キュー 2 が 75/ (25+75) です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

この例では、キュー 2 はキュー 1 の 3 倍の帯域幅を持っています。キュー 2 には、キュー 1 の 3 倍の頻度でサービスが提供されます。

次の例では、キューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/(4+4) です。SRR は最初、設定された 10% の帯域幅をキュー 1 (プライオリティ キュー) にサービスします。その後、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface [interface-id] queueing** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

#### 関連コマンド

| コマンド  | 説明   |
|---|--|
| <b>mls qos srr-queue input buffers</b>        | 入力キュー間のバッファを割り当てます。  |
| <b>mls qos srr-queue input cos-map</b>        | Class of Service (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。  |
| <b>mls qos srr-queue input dscp-map</b>       | DiffServ コードポイント (DSCP) 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。 |
| <b>mls qos srr-queue input priority-queue</b> | 入力プライオリティ キューを設定し、帯域幅を保証します。   |
| <b>mls qos srr-queue input threshold</b>      | Weighted Tail-Drop (WTD) しきい値のパーセンテージを入力キューに割り当てます。                      |
| <b>show mls qos input-queue</b>               | 入力キューの設定を表示します。  |
| <b>show mls qos interface queueing</b>        | Quality of Service (QoS) 情報を表示します。                                       |

# mls qos srr-queue input buffers

入力キュー間にバッファを割り当てるには、グローバル コンフィギュレーション モードで **mls qos srr-queue input buffers** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos srr-queue input buffers percentage1 percentage2
```

```
no mls qos srr-queue input buffers
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                    |  |
|--------------------|--|
| <i>percentage1</i> | 入力キュー 1 およびキュー 2 に割り当てられるバッファの割合 (%) です。 |
| <i>percentage2</i> | 指定できる範囲は 0 ~ 100 です。各値はスペースで区切ります。       |

## コマンドデフォルト

バッファの 90% がキュー 1 に、バッファの 10% がキュー 2 に割り当てられます。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。

## 例

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">mls qos srr-queue input bandwidth</a> | シェイプド ラウンドロビン (SRR) の重みを入力キューに割り当てます。                                    |
| <a href="#">mls qos srr-queue input cos-map</a>   | Class of Service (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。  |
| <a href="#">mls qos srr-queue input dscp-map</a>  | DiffServ コードポイント (DSCP) 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。 |

| コマンド  | 説明  |
|---|---|
| <code>mls qos srr-queue input priority-queue</code> | 入力プライオリティ キューを設定し、帯域幅を保証します。                        |
| <code>mls qos srr-queue input threshold</code>      | Weighted Tail-Drop (WTD) しきい値のパーセンテージを入力キューに割り当てます。 |
| <code>show mls qos input-queue</code>               | 入力キューの設定を表示します。                                     |
| <code>show mls qos interface buffers</code>         | Quality of Service (QoS) 情報を表示します。                  |

# mls qos srr-queue input cos-map

Class of Service (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングするには、グローバル コンフィギュレーション モードで **mls qos srr-queue input cos-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos srr-queue input cos-map queue queue-id {cos1...cos8 | threshold threshold-id
cos1...cos8}
```

```
no mls qos srr-queue input cos-map
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <b>queue</b> <i>queue-id</i>                               | キュー番号を指定します。<br><i>queue-id</i> で指定できる範囲は 1 ~ 2 です。   |
| <i>cos1...cos8</i>   | 入力キューにマッピングされた CoS 値。<br><i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。   |
| <b>threshold</b> <i>threshold-id</i><br><i>cos1...cos8</i> | CoS 値をキューのしきい値 ID にマッピングします。<br><i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。<br><i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。 |

## コマンドデフォルト

表 2-11 は、デフォルトの CoS 入力キューのしきい値マップを示しています。

表 2-11 デフォルトの CoS 入力キューしきい値

| CoS 値 | キュー ID - しきい値 ID |
|-------|------------------|
| 0 ~ 4 | 1 - 1            |
| 5     | 2 - 1            |
| 6、7   | 1 - 1            |

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

入力ポートに割り当てられた CoS によって、入力または出力のキューおよびしきい値が選択されます。しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。**mls qos srr-queue input threshold** グローバル コンフィギュレーション コマンドを使用すると、入力キューに 2 つの Weighted Tail-Drop (WTD) しきい値 (%) を割り当てることができます。

各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

**例**

次の例では、CoS 値 0～3 を、入力キュー 1 とドロップしきい値 50% のしきい値 ID 1 にマッピングする方法を示します。CoS 値 4 と 5 は、入力キュー 1 とドロップしきい値 70% のしきい値 ID 2 に割り当てます。

```
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 4 5
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

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

**関連コマンド**

| コマンド   | 説明   |
|--|--|
| <a href="#">mls qos srr-queue input bandwidth</a>      | シェイブド ラウンドロビン (SRR) の重みを入力キューに割り当てます。                                    |
| <a href="#">mls qos srr-queue input buffers</a>        | 入力キュー間のバッファを割り当てます。  |
| <a href="#">mls qos srr-queue input dscp-map</a>       | DiffServ コードポイント (DSCP) 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。 |
| <a href="#">mls qos srr-queue input priority-queue</a> | 入力プライオリティ キューを設定し、帯域幅を保証します。   |
| <a href="#">mls qos srr-queue input threshold</a>      | WTD しきい値のパーセンテージを入力キューに割り当てます。   |
| <a href="#">show mls qos maps</a>                      | QoS のマッピング情報を表示します。  |

# mls qos srr-queue input dscp-map

DiffServ コードポイント (DSCP) 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングするには、グローバル コンフィギュレーション モードで **mls qos srr-queue input dscp-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos srr-queue input dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id
dscp1...dscp8}
```

```
no mls qos srr-queue input dscp-map
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <b>queue</b> <i>queue-id</i>                                 | キュー番号を指定します。<br><i>queue-id</i> で指定できる範囲は 1 ~ 2 です。   |
| <i>dscp1...dscp8</i>   | 入力キューにマッピングする DSCP 値。<br><i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。   |
| <b>threshold</b> <i>threshold-id</i><br><i>dscp1...dscp8</i> | DSCP 値をキューしきい値 ID にマッピングします。<br><i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。<br><i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。 |

## コマンドデフォルト

表 2-12 は、デフォルトの DSCP 入力キューしきい値マップを示しています。

表 2-12 デフォルトの DSCP 入力キューしきい値マップ

| DSCP 値  | キュー ID - しきい値 ID |
|---------|------------------|
| 0 ~ 39  | 1 - 1            |
| 40 ~ 47 | 2 - 1            |
| 48 ~ 63 | 1 - 1            |

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン**

入力ポートに割り当てられた DSCP によって、入力または出力のキューおよびしきい値が選択されま  
す。

しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいつばい  
の状態に対して設定されます。 **mls qos srr-queue input threshold** グローバル コンフィギュレーショ  
ン コマンドを使用すると、入力キューに 2 つの Weighted Tail-Drop (WTD) しきい値 (%) を割り当  
てることができます。

各 DSCP 値を異なるキューおよびしきい値の組み合わせにマッピングして、フレームが別の方法で処  
理されるようにすることができます。

コマンドあたり最大 8 個の DSCP 値をマッピングできます。

**例**

次の例では、DSCP 値 0 ~ 6 を、入力キュー 1 とドロップしきい値 50% のしきい値 1 にマッピングす  
る方法を示します。DSCP 値 20 ~ 26 は、入力キュー 1 とドロップしきい値 70% のしきい値 2 にマッ  
ピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

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

**関連コマンド**

| コマンド  | 説明   |
|---|--|
| <b>mls qos srr-queue input bandwidth</b>      | シェイプド ラウンドロビン (SRR) の重みを入力<br>キューに割り当てます。                                      |
| <b>mls qos srr-queue input buffers</b>        | 入力キュー間のバッファを割り当てます。  |
| <b>mls qos srr-queue input cos-map</b>        | Class of Service (CoS) 値を入力キューにマッピングす<br>るか、CoS 値をキューおよびしきい値 ID にマッピング<br>します。 |
| <b>mls qos srr-queue input priority-queue</b> | 入力プライオリティ キューを設定し、帯域幅を保証し<br>ます。   |
| <b>mls qos srr-queue input threshold</b>      | WTD しきい値のパーセンテージを入力キューに割り当<br>てます。   |
| <b>show mls qos maps</b>                      | QoS のマッピング情報を表示します。  |

# mls qos srr-queue input priority-queue

リングが輻輳している場合、入力プライオリティ キューを設定し、内部リング上で帯域幅を保証するには、グローバル コンフィギュレーション モードで **mls qos srr-queue input priority-queue** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**mls qos srr-queue input priority-queue queue-id bandwidth weight**

**no mls qos srr-queue input priority-queue queue-id**



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                         |   |
|-------------------------|---|
| <i>queue-id</i>         | 入力のキュー ID。指定できる範囲は 1 ~ 2 です。                |
| <i>bandwidth weight</i> | 内部リングの帯域幅のパーセンテージを指定します。指定できる範囲は 0 ~ 40 です。 |

## コマンドデフォルト

プライオリティ キューはキュー 2 で、帯域幅の 10% が割り当てられています。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

プライオリティ キューは、優先して進める必要があるトラフィックに限り使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューは内部リング上で帯域幅の一部が保証されており、オーバーサブスクライプ型のリング上でネットワーク トラフィックが多い場合（バックプレーンが送達できる量よりもトラフィックが多い場合、およびキューがいっぱいでフレームをドロップしている場合）に、遅延とジッタを軽減します。

シェイプド ラウンドロビン (SRR) は、**mls qos srr-queue input priority-queue queue-id bandwidth weight** グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth weight1 weight2** グローバル コンフィギュレーション コマンドで設定された重みで指定した通りにサービスを行います。

プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、**mls qos srr-queue input priority-queue queue-id bandwidth 0** を入力します。

## 例

次の例では、キューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/(4+4) です。SRR は最初、設定された 10% の帯域幅をキュー 1 (プライオリティ キュー) にサービスします。その後、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

## 関連コマンド

| コマンド                                     | 説明  |
|--|---|
| <b>mls qos srr-queue input bandwidth</b> | シェイプド ラウンドロビン (SRR) の重みを入力キューに割り当てます。                                     |
| <b>mls qos srr-queue input buffers</b>   | 入力キュー間のバッファを割り当てます。   |
| <b>mls qos srr-queue input cos-map</b>   | Class of Service (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。   |
| <b>mls qos srr-queue input dscp-map</b>  | DiffServ コード ポイント (DSCP) 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。 |
| <b>mls qos srr-queue input threshold</b> | Weighted Tail-Drop (WTD) しきい値のパーセンテージを入力キューに割り当てます。                       |
| <b>show mls qos input-queue</b>          | 入力キューの設定を表示します。   |
| <b>show mls qos interface queueing</b>   | Quality of Service (QoS) 情報を表示します。  |

# mls qos srr-queue input threshold

入力キューに重み付けテールドロップ (WTD) しきい値のパーセンテージを割り当てるには、グローバル コンフィギュレーション モードで **mls qos srr-queue input threshold** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2
```

```
no mls qos srr-queue input threshold queue-id
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <i>queue-id</i>  | 入力キューの ID です。指定できる範囲は 1 ~ 2 です。   |
| <i>threshold-percentage1</i><br><i>threshold-percentage2</i> | 2 つの WTD しきい値 (%) です。各しきい値は、キューに割り当てられたキュー記述子の総数に対する割合です。各値はスペースで区切ります。指定できる範囲は 1 ~ 100 です。 |

## コマンド デフォルト

Quality of Service (QoS) がイネーブルなときは、WTD もイネーブルです。  
2 つの WTD しきい値は、100% に設定されます。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

QoS は、CoS/しきい値マップまたは DSCP/しきい値マップを使用して、どの Class of Service (CoS) 値または DiffServ コードポイント (DSCP) 値をしきい値 1 としきい値 2 にマッピングするかを判別します。しきい値 1 を超えた場合は、しきい値を超えなくなるまで、このしきい値に割り当てられた CoS または DSCP を持つパケットがドロップされます。ただし、しきい値 2 に割り当てられたパケットは、2 番めのしきい値を超えることがない限り、引き続きキューに入れられ送信されます。

各キューには、2 つの設定可能な (明示) ドロップしきい値と 1 つの事前設定された (暗黙) ドロップしきい値 (フル) があります。

CoS/しきい値マップを設定するには、**mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用します。DSCP/しきい値マップを設定するには、**mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。

## 例

次の例では、2 つのキューにテールドロップしきい値を設定する方法を示します。キュー 1 のしきい値は 50% と 100%、キュー 2 のしきい値は 70% と 100% です。

```
Switch(config)# mls qos srr-queue input threshold 1 50 100
Switch(config)# mls qos srr-queue input threshold 2 70 100
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <b>mls qos srr-queue input bandwidth</b>      | シェイプド ラウンドロビン (SRR) の重みを入力キューに割り当てます。                                     |
| <b>mls qos srr-queue input buffers</b>        | 入力キュー間のバッファを割り当てます。   |
| <b>mls qos srr-queue input cos-map</b>        | Class of Service (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。   |
| <b>mls qos srr-queue input dscp-map</b>       | DiffServ コード ポイント (DSCP) 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。 |
| <b>mls qos srr-queue input priority-queue</b> | 入力プライオリティ キューを設定し、帯域幅を保証します。  |
| <b>show mls qos input-queue</b>               | 入力キューの設定を表示します。   |
| <b>show mls qos interface buffers</b>         | Quality of Service (QoS) 情報を表示します。  |

# mls qos srr-queue output cos-map

Class of Service (CoS) 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングするには、グローバル コンフィギュレーション モードで **mls qos srr-queue output cos-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos srr-queue output cos-map queue queue-id {cos1...cos8 | threshold threshold-id
cos1...cos8}
```

```
no mls qos srr-queue output cos-map
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <b>queue</b> <i>queue-id</i>                               | キュー番号を指定します。<br><i>queue-id</i> で指定できる範囲は 1 ~ 4 です。   |
| <i>cos1...cos8</i>   | 出力キューにマッピングされた CoS 値。<br><i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。   |
| <b>threshold</b> <i>threshold-id</i><br><i>cos1...cos8</i> | CoS 値をキューのしきい値 ID にマッピングします。<br><i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。<br><i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。 |

## コマンドデフォルト

表 2-13 は、デフォルトの CoS 出力キューのしきい値マップを示しています。

表 2-13 デフォルトの CoS 出力キューしきい値マップ

| CoS 値 | キュー ID - しきい値 ID |
|-------|------------------|
| 0、1   | 2 - 1            |
| 2、3   | 3 - 1            |
| 4     | 4 - 1            |
| 5     | 1 - 1            |
| 6、7   | 4 - 1            |

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいつばいの状態に対して設定されます。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの Quality of Service (QoS) ソリューションを満たさないと判断した場合に限り、設定を変更することができます。

**mls qos queue-set output *qset-id* threshold** グローバル コンフィギュレーション コマンドを使用すると、出力キューに 2 つの Weighted Tail-Drop (WTD) しきい値 (%) を割り当てることができます。各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

## 例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。CoS 値 0 ~ 3 を出力キュー 1 としきい値 ID 1 にマッピングします。キュー 1 のドロップしきい値を割り当てられたメモリの 50% と 70% に設定し、割り当てられたメモリの 100% を保証 (予約) して、このキューがパケットをドロップせずに保持できる最大メモリを 200% に設定します。

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface [*interface-id*] buffers**、または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                      | 説明  |
|---|---|
| <b>mls qos queue-set output threshold</b> | WTD しきい値を設定して、バッファのアベイラビリティを保証し、キューセットへの最大メモリ割り当てを設定します。  |
| <b>mls qos srr-queue output dscp-map</b>  | Diffserv コードポイント (DSCP) 値を出力キュー、またはキューとしきい値 ID にマッピングします。 |
| <b>queue-set</b>                          | ポートをキューセットにマッピングします。                                      |
| <b>show mls qos interface buffers</b>     | QoS 情報を表示します。   |
| <b>show mls qos maps</b>                  | QoS のマッピング情報を表示します。                                       |
| <b>show mls qos queue-set</b>             | キューセットの出力キューセット値を表示します。                                   |

# mls qos srr-queue output dscp-map

DiffServ コードポイント (DSCP) 値を出力キューにマッピングするか、または DSCP 値をキューとしきい値 ID 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 **mls qos srr-queue output dscp-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id
dscp1...dscp8}
```

```
no mls qos srr-queue output dscp-map
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <b>queue</b> <i>queue-id</i>                                 | キュー番号を指定します。<br><i>queue-id</i> で指定できる範囲は 1 ~ 4 です。   |
| <i>dscp1...dscp8</i>   | 出力キューにマッピングする DSCP 値。<br><i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。   |
| <b>threshold</b> <i>threshold-id</i><br><i>dscp1...dscp8</i> | DSCP 値をキューしきい値 ID にマッピングします。<br><i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。<br><i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。 |

## コマンドデフォルト

表 2-14 は、デフォルトの DSCP 出力キューしきい値マップを示しています。

表 2-14 デフォルトの DSCP 出力キューしきい値マップ

| DSCP 値  | キュー ID - しきい値 ID |
|---------|------------------|
| 0 ~ 15  | 2 - 1            |
| 16 ~ 31 | 3 - 1            |
| 32 ~ 39 | 4 - 1            |
| 40 ~ 47 | 1 - 1            |
| 48 ~ 63 | 4 - 1            |

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいつばいの状態に対して設定されます。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

**mls qos queue-set output *qset-id* threshold** グローバル コンフィギュレーション コマンドを使用すると、出力キューに 2 つの Weighted Tail-Drop (WTD) しきい値 (%) を割り当てることができます。

各 DSCP 値を異なるキューおよびしきい値の組み合わせにマッピングして、フレームが別の方法で処理されるようにすることができます。

コマンドあたり最大 8 個の DSCP 値をマッピングできます。

## 例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。DSCP 値 0 ~ 3 を出力キュー 1 としきい値 ID 1 にマッピングします。キュー 1 のドロップしきい値を割り当てられたメモリの 50% と 70% に設定し、割り当てられたメモリの 100% を保証 (予約) して、このキューがパケットをドロップせずに保持できる最大メモリを 200% に設定します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface [*interface-id*] buffers**、または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                      | 説明   |
|---|--|
| <b>mls qos queue-set output threshold</b> | WTD しきい値を設定して、バッファの可用性を保証し、キューセットへの最大メモリ割り当てを設定します。      |
| <b>mls qos srr-queue output cos-map</b>   | Class of Service (CoS) 値を出力キュー、またはキューとしきい値 ID にマッピングします。 |
| <b>queue-set</b>                          | ポートをキューセットにマッピングします。                                     |
| <b>show mls qos interface buffers</b>     | Quality of Service (QoS) 情報を表示します。                       |
| <b>show mls qos maps</b>                  | QoS のマッピング情報を表示します。                                      |
| <b>show mls qos queue-set</b>             | キューセットの出力キューセット値を表示します。                                  |

# mls qos trust

ポートの信頼状態を設定するには、インターフェイス コンフィギュレーション モードで **mls qos trust** コマンドを使用します。ポートを信頼できない状態に戻すには、このコマンドの **no** 形式を使用します。

**mls qos trust [cos | device cisco-phone | dscp | ip-precedence]**

**no mls qos trust [cos | device | dscp | ip-precedence]**



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                           |  |
|---------------------------|--|
| <b>cos</b>                | (任意) パケットの CoS 値を使用して、入力パケットを分類します。タグのないパケットについては、ポートのデフォルト CoS 値を使用します。   |
| <b>device cisco-phone</b> | (任意) 信頼設定に応じて、Cisco IP Phone (信頼される境界) から送信された CoS または DSCP 値を信頼することにより入力パケットを分類します。   |
| <b>dscp</b>               | (任意) パケット DSCP 値 (8 ビット サービスタイプ フィールドの上位 6 ビット) を使用して、入力パケットを分類します。非 IP パケットでパケットがタグ付きの場合は、パケット CoS が使用されます。タグなしパケットの場合は、デフォルトのポート CoS 値が使用されます。               |
| <b>ip-precedence</b>      | (任意) パケット IP-precedence 値 (8 ビット サービスタイプ フィールドの上位 3 ビット) を使用して、入力パケットを分類します。非 IP パケットでパケットがタグ付きの場合は、パケット CoS が使用されます。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。 |

## コマンド デフォルト

ポートは信頼されていません。キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** です。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

入力トラフィックを信頼できるようになり、パケットの Diffserv コード ポイント (DSCP)、Class of Service (CoS)、または IP precedence のフィールドを調べることにより分類が実行されます。

Quality of Service (QoS) ドメインに着信するパケットは、ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートはいずれか 1 つの信頼状態に設定できます。ポートが信頼されているかどうか、またどのパケットのフィールドがトラフィックの分類に使用されるのかを指定する場合に、このコマンドを使用します。

ポートに信頼 DSCP または信頼 IP precedence が設定され、着信パケットが非 IP パケットの場合は、CoS/DSCP マップを使用して、CoS 値から対応する DSCP 値が導き出されます。CoS は、トランクポートの場合はパケット CoS、非トランクポートの場合はデフォルトのポート CoS となります。

DSCP が信頼されている場合、IP パケットの DSCP フィールドは変更されません。ただし、パケットの CoS 値を (DSCP/CoS マップに基づいて) 変更することは可能です。

CoS が信頼されている場合、パケットの CoS フィールドは変更されませんが、IP パケットである場合には (CoS/DSCP マップに基づいて) DSCP を変更することはできません。

信頼境界機能は、ユーザがネットワーク化された Cisco IP Phone から PC を切断し、これをスイッチポートに接続して信頼された CoS または DSCP 設定を利用する場合のセキュリティ問題の発生を防止します。スイッチおよび IP Phone に接続されたポートで Cisco Discovery Protocol (CDP) をグローバルにイネーブルにする必要があります。IP Phone が検出されなかった場合、信頼境界機能はスイッチまたはルーテッドポートの信頼設定をディセーブルにし、高プライオリティ キューが誤って使用されないようにします。

DSCP または IP precedence の信頼設定を行うと、着信パケットの DSCP 値または IP precedence 値が信頼されます。IP Phone に接続するスイッチポートで **mls qos cos override** インターフェイス コンフィギュレーション コマンドを設定すると、スイッチは着信音声およびデータパケットの CoS を無効にし、デフォルトの CoS 値をそれらに割り当てます。

QoS ドメイン間境界の場合は、ポートを DSCP 信頼状態に設定し、DSCP 値が QoS ドメイン間で異なる場合は DSCP/DSCP 変換マップを適用することができます。

ポート信頼状態を使用した分類 (たとえば、**mls qos trust [cos | dscp | ip-precedence]**) とポリシーマップ (たとえば、**service-policy input policy-map-name**) は同時に指定できません。最後に行われた設定により、前の設定が上書きされます。



(注)

Cisco IOS Release 15.0(1)EY 以降では、デュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを持つ IPv6 ポート ベースのトラストをサポートしています。IPv6 が動作しているスイッチのデュアル IPv4/IPv6 テンプレートを持つスイッチをリロードする必要があります。

## 例

次の例では、着信パケットの IP precedence フィールドを信頼するようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust ip-precedence
```

次の例では、ポートに接続している Cisco IP Phone が信頼できる装置であると指定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust device cisco-phone
```

**show mls qos interface** 特権 EXEC コマンドを入力すると、設定を確認できます。

## 関連コマンド

| コマンド                          | 説明   |
|-------------------------------|--|
| <b>mls qos cos</b>            | デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。                              |
| <b>mls qos dscp-mutation</b>  | DSCP/DSCP 変換マップを DSCP の信頼できるポートに適用します。   |
| <b>mls qos map</b>            | CoS/DSCP マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシー設定 DSCP マップを定義します。 |
| <b>show mls qos interface</b> | QoS 情報を表示します。  |

# mls qos vlan-based

物理ポートで VLAN ベースの Quality Of Service (QoS) をイネーブルにするには、インターフェイス コンフィギュレーション モードで **mls qos vlan-based** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**mls qos vlan-based**

**no mls qos vlan-based**



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 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 デフォルト

VLAN ベースの QoS はディセーブルです。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

階層ポリシー マップをスイッチ仮想インターフェイス (SVI) に適用するには、階層ポリシー マップのセカンダリ インターフェイス レベルでポートを指定するときに、物理ポートで **mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用します。

階層ポリシーを設定すると、階層ポリシー マップは SVI に適用され、VLAN に属するすべてのトラフィックに反映されます。インターフェイス レベルのトラフィック分類における個々のポリサーは、分類に従って指定された物理ポートだけに反映されます。

階層型ポリシー マップを設定する詳細な手順については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Classifying, Policing, and Marking Traffic by Using Hierarchical Policy Maps」の項を参照してください。

## 例

次の例では、物理ポート上で VLAN ベースのポリシーをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos vlan-based
```

**show mls qos interface** 特権 EXEC コマンドを入力すると、設定を確認できます。

## 関連コマンド

| コマンド                                   | 説明            |
|--|---------------|
| <a href="#">show mls qos interface</a> | QoS 情報を表示します。 |

# 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) の宛先ポート上で入力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、グローバル コンフィギュレーション モードで **monitor session** 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に対してこのコマンドの **no** 形式を使用すると、カプセル化オプションは無視されます。

```
monitor session session_number destination {interface interface-id [, | -] [encapsulation {dot1q | replicate}] [ingress {dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id}] | {remote vlan vlan-id}
```

```
monitor session session_number filter vlan vlan-id [, | -]
```

```
monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan vlan-id [, | -] [both | rx | tx]} | {remote vlan vlan-id}
```

```
no monitor session {session_number | all | local | remote}
```

```
no monitor session session_number destination {interface interface-id [, | -] [encapsulation {dot1q | replicate}] [ingress {dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id}] | {remote vlan vlan-id}
```

```
no monitor session session_number filter vlan vlan-id [, | -]
```

```
no monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan vlan-id [, | -] [both | rx | tx]} | {remote vlan vlan-id}
```

## 構文の説明

|                                       |  |
|---------------------------------------|--|
| <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。  |
| <b>destination</b>                    | 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。   |
| <b>interface</b> <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。 <b>送信元インターフェイス</b> の場合は、 <b>ポートチャネル</b> 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 ~ 6 です。                           |
| <b>encapsulation</b> <b>dot1q</b>     | (任意) 宛先インターフェイスが IEEE 802.1Q カプセル化方式を使用することを指定します。<br><br>次のキーワードは、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。                                    |
| <b>encapsulation</b> <b>replicate</b> | (任意) 宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。<br><br>次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。 |
| <b>ingress</b>                        | (任意) 入力トラフィック転送をイネーブルにします。   |

|                                     |  |
|-------------------------------------|--|
| <b>dot1q vlan</b> <i>vlan-id</i>    | デフォルト VLAN として指定された VLAN で IEEE 802.1Q カプセル化を持つ着信パケットを受け入れます。  |
| <b>untagged vlan</b> <i>vlan-id</i> | デフォルト VLAN として指定された VLAN でタグなしカプセル化を持つ着信パケットを受け入れます。   |
| <b>vlan</b> <i>vlan-id</i>          | <b>ingress</b> 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。  |
| <b>remote vlan</b> <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。<br><br>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。   |
| <b>filter vlan</b> <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。  |
| <b>source</b>                       | 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。  |
| <b>both、rx、tx</b>                   | (任意) モニタ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。  |
| <b>source vlan</b> <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。  |
| <b>all、local、remote</b>             | 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、 <b>no monitor session</b> コマンドに <b>all、local、remote</b> を指定します。  |

**コマンド デフォルト**

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタリングします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。

ローカル SPAN の宛先ポートで **encapsulation replicate** が指定されなかった場合、パケットはカプセル化のタグなしのネイティブ形式で送信されます。

入力転送は宛先ポートではディセーブルになっています。

**コマンド モード**

グローバル コンフィギュレーション

**コマンド履歴**

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

個々のポートはそれらが EtherChannel に参加している間もモニタリングすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタリングすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1x 認証をイネーブルにすることはできませんが、ポートが SPAN 宛先として削除されるまで IEEE 802.1x 認証はディセーブルです。IEEE 802.1x 認証がポート上で使用できない場合、スイッチはエラー メッセージを返します。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワーク トラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信元ポートでモニタリングされます。**monitor session session\_number filter vlan vlan-id** コマンドを使用すると、トランク送信元ポートの SPAN トラフィックを指定された VLAN だけに限定できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLAN のフィルタリングはイネーブルにできません。VLAN のフィルタリングが設定されている場合、VLAN は送信元になることができません。

入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- 他のキーワードなしで、**monitor session session\_number destination interface interface-id** を入力した場合、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session session\_number destination interface interface-id ingress** を入力した場合は、出力カプセル化はタグなしで、入力カプセル化はそのあとに続くキーワードが **dot1q**、**untagged** のいずれであるかによって決まります。

- 他のキーワードを指定せずに **monitor session session\_number destination interface interface-id encapsulation dot1q** を入力すると、出力カプセル化で IEEE 802.1Q カプセル化方式が使用されます（これは、ローカル SPAN だけに適用されます。RSPAN は **dot1q カプセル化** をサポートしていません）。
- **monitor session session\_number destination interface interface-id encapsulation dot1q ingress** を入力した場合は、出力カプセル化には IEEE 802.1Q カプセル化が使用され、入力カプセル化はそのあとに続くキーワードが、**dot1q** または **untagged** のいずれであるかによって決まります（これは、ローカル SPAN だけに適用されます。RSPAN は **dot1q カプセル化** をサポートしていません）。
- 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あとに続くキーワードが、**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）。

## 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 gigabitethernet1/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/2
```

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 gigabitethernet1/2
```

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 gigabitethernet1/1
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 gigabitethernet1/2
```

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 gigabitethernet1/2 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 gigabitethernet1/2 ingress  
untagged vlan 5
```

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN および RSPAN 設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

#### 関連コマンド

| コマンド                                | 説明  |
|-------------------------------------|---|
| <a href="#">remote-span</a>         | vlan コンフィギュレーション モードで RSPAN VLAN を設定します。  |
| <a href="#">show monitor</a>        | SPAN および RSPAN セッション情報を表示します。   |
| <a href="#">show running-config</a> | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

## mvr (グローバル コンフィギュレーション)

スイッチ上でルチキャスト 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グローバル コンフィギュレーション モードで **mvr** 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 メンバーシップからのポートの削除を行う前に、クエリーの返答を待つ最大時間の設定、または MVR マルチキャスト VLAN の指定が行われます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mvr [group ip-address [count] | mode [compatible | dynamic] | querytime value | vlan vlan-id]
```

```
no mvr [group ip-address | mode [compatible | dynamic] | querytime value | vlan vlan-id]
```

### 構文の説明

|                         |   |
|-------------------------|---|
| <b>group ip-address</b> | (任意) 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。<br><br>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 <b>no</b> 形式を使用します。   |
| <b>count</b>            | (任意) 複数の連続する MVR グループ アドレスを設定します。指定できる範囲は 1 ~ 256 です。デフォルト値は 1 です。  |
| <b>mode</b>             | (任意) MVR の動作モードを指定します。<br><br>デフォルトは <b>compatible</b> モードです。   |
| <b>compatible</b>       | (任意) 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 メンバーシップ加入は使用できません。   |
| <b>dynamic</b>          | (任意) MVR モードを設定して、送信元ポートでダイナミック MVR メンバーシップを使用できるようにします。  |
| <b>querytime value</b>  | (任意) レシーバポートで IGMP レポート メンバー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 メンバーシップ 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 メンバーシップから削除します。<br><br>この値は 10 分の 1 秒単位の応答時間です。指定できる範囲は 1 ~ 100 です。デフォルトは 5/10 秒つまり 1/2 秒です。<br><br>デフォルト設定に戻す場合は、このコマンドの <b>no</b> 形式を使用します。 |
| <b>vlan vlan-id</b>     | (任意) MVR マルチキャスト データの受信が予想される VLAN を指定します。これは、すべての送信元ポートが属する VLAN でもあります。指定できる範囲は 1 ~ 4094 です。デフォルト値は VLAN 1 です。  |

### コマンド デフォルト

MVR はデフォルトでディセーブルです。

デフォルトの MVR モードは、**compatible** モードです。

IP マルチキャスト アドレスは、デフォルトではスイッチで設定されます。

デフォルトのグループ IP アドレス カウントは 0 です。

デフォルトのクエリー応答時間は 5/10 秒つまり 1/2 秒です。

デフォルトの MVR 用マルチキャスト VLAN は VLAN 1 です。

**コマンドモード** グローバル コンフィギュレーション

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン** 最大 256 の MVR マルチキャスト グループを 1 つのスイッチで設定できます。

MVR に属するすべての IP マルチキャスト アドレスをスタティックに設定する場合は、**mvr group** コマンドを使用します。設定したマルチキャスト アドレスに送信されたマルチキャスト データは、スイッチのすべての送信元ポートおよびその IP マルチキャスト アドレスでデータを受信するよう登録されたすべてのレシーバ ポートに送信されます。

MVR はスイッチのエイリアス IP マルチキャスト アドレスをサポートします。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス (224.0.0.xxx 範囲内) を設定する必要はありません。

**mvr querytime** コマンドはレシーバ ポートだけに適用されます。

スイッチ MVR が、Catalyst 2900 XL または Catalyst 3500 XL スイッチと相互動作している場合は、マルチキャスト モードを **compatible** に設定してください。

**compatible** モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR はスイッチで IGMP スヌーピングと共存できます。

マルチキャスト ルーティングおよび MVR はスイッチ上で共存できません。MVR がイネーブルになっている状態で、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにした場合、MVR はディセーブルになり、警告メッセージが表示されます。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの状態、MVR をイネーブルにしようとする、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
```

スイッチで設定された IP マルチキャスト グループ アドレスを表示する場合は、**show mvr members** 特権 EXEC コマンドを使用します。

## ■ mvr (グローバル コンフィギュレーション)

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
```

## 関連コマンド

| コマンド                              | 説明   |
|-----------------------------------|--|
| <b>mvr</b> (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。   |
| <b>show mvr</b>                   | 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。   |
| <b>show mvr interface</b>         | 設定された MVR インターフェイスをそのタイプ、ステータス、および即時脱退設定とともに表示します。インターフェイスがメンバであるすべての MVR グループを表示します。  |
| <b>show mvr members</b>           | 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 <b>Inactive</b> 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、インターフェイス コンフィギュレーション モードで **mvr** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mvr [immediate | type {receiver | source} | vlan vlan-id group [ip-address]]
```

```
no mvr [immediate | type {source | receiver} | vlan vlan-id group [ip-address]]
```

### 構文の説明

|                           |   |
|---------------------------|---|
| <b>immediate</b>          | (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、 <b>no mvr immediate</b> コマンドを使用します。   |
| <b>type</b>               | (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。<br><br>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。 <b>no mvr type</b> 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。 |
| <b>receiver</b>           | 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。受信ポートをマルチキャスト VLAN に所属させることはできません。  |
| <b>source</b>             | 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。   |
| <b>vlan vlan-id group</b> | (任意) ポートを、指定された VLAN ID を持つマルチキャストグループのスタティック メンバとして追加します。<br><br><b>no mvr vlan vlan-id group</b> コマンドは、IP マルチキャスト アドレス グループのメンバーシップから VLAN 上のポートを削除します。             |
| <b>ip-address</b>         | (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 アドレスを静的に設定します。これは、ポートが加入しているマルチキャスト グループの IP アドレスです。   |

### コマンド デフォルト

ポートはレシーバとしても送信元としても設定されません。

即時脱退機能はすべてのポートでディセーブルです。

レシーバ ポートはどの設定済みマルチキャスト グループにも属していません。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

ポートが設定されたマルチキャスト グループ向けマルチキャスト データを送受信できるようにする場合は、ポートを送信元ポートとして設定します。マルチキャスト データは送信元ポートとして設定されているすべてのポートで受信されます。

レシーバ ポートはトランク ポートになることはできません。スイッチのレシーバ ポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。

MVR に参加していないポートは、MVR レシーバ ポートまたは送信元ポートとして設定しないでください。非 MVR ポートは通常のスイッチ ポートであり、通常のスイッチ動作でマルチキャスト データを送受信することができます。

即時脱退機能がイネーブルの場合、レシーバ ポートはより短時間でマルチキャスト グループから脱退します。即時脱退機能がなく、スイッチがレシーバ ポートのグループから IGMP Leave メッセージを受信した場合、スイッチは、そのポートに IGMP MAC (メディア アクセス コントロール) ベースのクエリを送信し、IGMP グループ メンバーシップ レポートを待ちます。設定された時間内にレポートを受信しなかった場合は、受信ポートがマルチキャスト グループ メンバー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、受信ポートがマルチキャスト グループ メンバーシップから削除されるので、脱退遅延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。

## 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 gigabitethernet1/2
Switch(config-if)# mvr type receiver
```

設定されたレシーバ ポートおよび送信元ポートを表示するには、**show mvr interface** 特権 EXEC コマンドを使用します。

次の例では、ポートの即時脱退機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mvr immediate
```

次の例では、VLAN 1 のポートを IP マルチキャスト グループ 228.1.23.4 のスタティック メンバとして追加する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

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

## 関連コマンド

| コマンド                                 | 説明   |
|--------------------------------------|--|
| <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>show mvr</code>                | 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。   |
| <code>show mvr interface</code>      | 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。 |
| <code>show mvr members</code>        | MVR マルチキャスト グループのメンバであるすべてのレシーバポートを表示します。  |

# network-policy

インターフェイスにネットワーク ポリシー プロファイルを適用するには、インターフェイス コンフィギュレーション モードで **network-policy** コマンドを使用します。ポリシーを削除する場合は、このコマンドの **no** 形式を使用します。

**network-policy** *profile number*

**no network-policy**

## 構文の説明

*profile number* ネットワーク ポリシー プロファイル番号。

## コマンドデフォルト

ネットワークポリシー プロファイルは適用されません。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

インターフェイスにプロファイルを適用するには、**network-policy profile number** インターフェイス コンフィギュレーション コマンドを使用します。

最初にインターフェイス上にネットワークポリシー プロファイルを設定した場合、インターフェイス上に **switchport voice vlan** コマンドを適用できません。 **switchport voice vlan vlan-id** がすでにインターフェイス上に設定されている場合、ネットワークポリシー プロファイルをインターフェイス上に適用できます。その後、インターフェイスは、インターフェイス上に適用された音声または音声シグナリング VLAN ネットワークポリシー プロファイルを使用します。

## 例

次の例では、インターフェイスにネットワークポリシー プロファイル 60 を適用する方法を示します。

```
Switch(config)# interface_id
Switch(config-if)# network-policy profile 60
```

## 関連コマンド

| コマンド   | 説明                            |
|--|-------------------------------|
| <b>network-policy profile</b> (グローバル コンフィギュレーション)      | ネットワークポリシー プロファイルを作成します。      |
| <b>network-policy profile</b> (ネットワークポリシー コンフィギュレーション) | ネットワークポリシー プロファイルの属性を設定します。   |
| <b>show network-policy profile</b>                     | 設定されたネットワークポリシー プロファイルを表示します。 |

# network-policy profile (グローバル コンフィギュレーション)

ネットワークポリシー プロファイルを作成し、ネットワークポリシー コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **network-policy profile** コマンドを使用します。ポリシーを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

**network-policy profile profile number**

**no network-policy profile profile number**

## 構文の説明

*profile number* ネットワーク ポリシー プロファイル番号を指定します。指定できる範囲は 1 ~ 4294967295 です。

## コマンド デフォルト

ネットワークポリシー プロファイルは定義されていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードに入るには、**network-policy profile** グローバル コンフィギュレーション コマンドを使用します。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service (CoS)、DiffServ コード ポイント (DSCP) の値、およびタギング モードを指定することで、音声および音声シグナリング用のプロファイルを作成することができます。

その後、これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) の **network-policy** Time Length Value (TLV) に含まれます。

## 例

次の例では、ネットワークポリシー プロファイル 60 を作成する方法を示します。

```
Switch(config)# network-policy profile 60
Switch(config-network-policy)#
```

## ■ network-policy profile (グローバル コンフィギュレーション)

| 関連コマンド | コマンド  | 説明                            |
|--------|---|-------------------------------|
|        | <a href="#">network-policy</a>                                  | インターフェイスにネットワークポリシーを適用します。    |
|        | <a href="#">network-policy profile (ネットワークポリシー コンフィギュレーション)</a> | ネットワークポリシー プロファイルの属性を設定します。   |
|        | <a href="#">show network-policy profile</a>                     | 設定されたネットワークポリシー プロファイルを表示します。 |

# network-policy profile (ネットワークポリシー コンフィギュレーション)

ネットワーク ポリシー プロファイルを設定するには、グローバル コンフィギュレーション モードで **network-policy profile** を使用します。プロファイルを削除する場合は、追加パラメータなしでこのコマンドの **no** 形式を使用します。設定された属性を変更する場合は、パラメータとともにこのコマンドの **no** 形式を使用します。

```
network-policy profile profile number {voice | voice-signaling} vlan [vlan-id {cos cvalue | dscp dvalue}] | [[dot1p {cos cvalue | dscp dvalue}] | none | untagged]
```

```
no network-policy profile profile number {voice | voice-signaling} vlan [vlan-id {cos cvalue} | {dscp dvalue}] | [[dot1p {cos cvalue} | {dscp dvalue}] | none | untagged]
```

## 構文の説明

|                        |  |
|------------------------|--|
| <b>voice</b>           | 音声アプリケーションタイプを指定します。   |
| <b>voice-signaling</b> | 音声シグナリング アプリケーションタイプを指定します。  |
| <b>vlan</b>            | 音声トラフィック用のネイティブ VLAN を指定します。   |
| <b>vlan-id</b>         | (任意) 音声トラフィック用の VLAN を指定します。指定できる範囲は 1 ~ 4094 です。  |
| <b>cos cvalue</b>      | (任意) 設定された VLAN に対するレイヤ 2 プライオリティ Class of Service (CoS) を指定します。指定できる範囲は 0 ~ 7 です。デフォルトは 0 です。 |
| <b>dscp dvalue</b>     | (任意) 設定された VLAN に対する Diffserv コードポイント (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 です。デフォルトは 0 です。           |
| <b>dot1p</b>           | (任意) IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように電話を設定します。                         |
| <b>none</b>            | (任意) 音声 VLAN に関して IP Phone に指示しません。IP Phone のキーパッドから入力された設定を使用します。                             |
| <b>untagged</b>        | (任意) IP Phone をタグなしの音声トラフィックを送信するよう設定します。これが IP Phone のデフォルト設定になります。                           |

## コマンド デフォルト

ネットワーク ポリシーは定義されていません。

## コマンド モード

ネットワークポリシー コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

ネットワークポリシー プロファイルの属性を設定するには、**network-policy profile** コマンドを使用します。

**voice** アプリケーションタイプは IP Phone 専用であり、対話形式の音声サービスをサポートするデバイスに似ています。通常、これらのデバイスは、展開を容易に行えるようにし、データアプリケーションから隔離してセキュリティを強化するために、別個の VLAN に配置されます。

## network-policy profile (ネットワークポリシー コンフィギュレーション)

**voice-signaling** アプリケーション タイプは、音声メディアと異なる音声シグナリング用のポリシーを必要とするネットワーク トポロジ用です。すべての同じネットワーク ポリシーが **voice policy** TLV にアドバタイズされたポリシーとして適用される場合、このアプリケーション タイプはアドバタイズしないでください。

次の例では、プライオリティ 4 の CoS を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
```

次の例では、DSCP 値 34 を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 dscp 34
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
```

## 関連コマンド

| コマンド   | 説明                            |
|--|-------------------------------|
| <a href="#">network-policy</a>                             | インターフェイスにネットワークポリシーを適用します。    |
| <a href="#">network-policy profile (グローバル コンフィギュレーション)</a> | ネットワークポリシー プロファイルを作成します。      |
| <a href="#">show network-policy profile</a>                | 設定されたネットワークポリシー プロファイルを表示します。 |

# nmosp

スイッチのネットワーク モビリティ サービス プロトコル (NMSP) をイネーブルにするには、グローバル コンフィギュレーション モードで **nmosp** を使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
nmosp {enable | {notification interval {attachment | location} interval-seconds}}
```

```
no nmosp {enable | {notification interval {attachment | location} interval-seconds}}
```

## 構文の説明

|                              |  |
|------------------------------|--|
| <b>enable</b>                | スイッチで NMSP 機能をイネーブルにします。   |
| <b>notification interval</b> | NMSP 通知間隔を指定します。   |
| <b>attachment</b>            | 接続通知間隔を指定します。  |
| <b>location</b>              | ロケーション通知間隔を指定します。  |
| <i>interval-seconds</i>      | スイッチが MSE にロケーションまたはアタッチメントの更新を送信するまでの期間 (秒)。指定できる範囲は 1 ~ 30 です。デフォルト値は 30 です。 |

## コマンドデフォルト

NMSP はディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

NMSP ロケーションおよびアタッチメント通知を Cisco Mobility Services Engine (MSE) に送信するようにスイッチをイネーブルにするには、**nmosp** グローバル コンフィギュレーション コマンドを使用します。

## 例

次の例では、スイッチ上で NMSP をイネーブルにし、ロケーション通知時間を 10 秒に設定する方法を示します。

```
Switch(config)# vlan enable
Switch(config)# vlan notification interval location 10
```

## 関連コマンド

| コマンド                                      | 説明                                  |
|---|-------------------------------------|
| <a href="#">clear nmosp statistics</a>    | NMSP 統計カウンタをクリアします。                 |
| <a href="#">nmosp attachment suppress</a> | 特定のインターフェイスからのアタッチメント情報のレポートを抑制します。 |
| <a href="#">show nmosp</a>                | NMSP 情報を表示します。                      |

# nmsp attachment suppress

特定のインターフェイスからのアタッチメント情報のレポートを抑制するには、インターフェイス コンフィギュレーション モードで **nmsp attachment suppress** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**nmsp attachment suppress**

**no nmsp attachment suppress**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

なし

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

ロケーションおよびアタッチメント通知を Cisco Mobility Services Engine (MSE) に送信しないようにインターフェイスを設定するには、**nmsp attachment suppress** インターフェイス コンフィギュレーション コマンドを使用します。

## 例

次の例では、アタッチメント情報を MSE に送信しないようにインターフェイスを設定する方法を示します。

```
Switch(config)# switch interface interface-id
Switch(config-if)# nmsp attachment suppress
```

## 関連コマンド

| コマンド             | 説明   |
|------------------|--|
| <b>nmsp</b>      | スイッチ上でネットワーク モビリティ サービス プロトコル (NMSP) をイネーブルにします。 |
| <b>show nmsp</b> | NMSP 情報を表示します。                                   |

# outside from

内部アドレスに外部アドレスを変換するには、config l2nat モードで **outside from** コマンドを使用します。

変換を削除するには、このコマンドの **no** 形式を入力します。

```
outside from {host | range | network} original ip/ip subnet to translated ip/ip subnet [mask]
            number | mask
```

```
no outside from {host | range | network} original ip/ip subnet to translated ip/ip subnet [mask]
            number|mask
```

## 構文の説明

|                                     |  |
|-------------------------------------|--|
| <b>host</b>                         | 単一のホスト アドレスを変換します。   |
| <b>range</b>                        | ホスト アドレス範囲を変換します。 <i>number</i> を入力して範囲のサイズを指定します。   |
| <b>network</b>                      | サブネット内のすべてのホスト アドレスを変換します。ホストのオクテットは 1.1.0.0 のように 0 にする必要があります。別の値を入力した場合、無視されます。 <i>translated ip</i> を入力する場合、 <b>mask mask</b> を含めます。                  |
| <i>original ip to translated ip</i> | ホスト、範囲、ネットワークのパブリック IP アドレスと、対応するプライベート IP アドレス。   |
| <b>mask mask</b>                    | <b>network</b> オプションを使用する場合以外は任意です。サブネット マスク。有効なサブネットは 255.255.0.0、255.255.255.0、255.255.255.128、255.255.255.192、255.255.255.224、および 255.255.255.240 です。 |
| <i>number</i>                       | <b>range</b> オプションを使用する場合以外は任意です。範囲のサイズ。   |

## コマンド デフォルト

なし

## コマンド モード

Config-l2nat

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(2)EB | このコマンドが導入されました。 |

## 使用上のガイドライン

- 各レイヤ 2 NAT インスタンスの変換を設定します。
- 内部ネットワークのデバイスから外部ネットワーク デバイスに ping を実行するには、外部デバイスの変換済みアドレスを使用します。たとえば、外部ホスト 10.10.10.1 から内部ホスト 192.168.1.1 に変換される場合は、ping 192.168.1.1 です。
- レイヤ 2 NAT インスタンスがすでにある場合、新しい変換値は前述のリストに追加されます。
- 範囲：
  - 範囲は互いに重複させないでください。
  - 範囲は /24 のネットワーク設定と重複させないでください。
  - オリジナルと変換された IP アドレスは 1 対 1 に対応させる必要があります (x.x.x.1 ~ y.y.y.1、x.x.x.2 ~ x.x.x.2 など)。元のアドレスおよび変換されたアドレスがこのように対応していない場合は、**host** コマンドを使用して各アドレスを個別に設定できます。

## ■ outside from

## 例

次に、外部アドレス 10.1.0.100 から内部アドレス 192.168.0.100 に変換するように Instance1 という名前のインスタンスを設定する例を示します。

```
Switch(config)# l2nat instance Instance1
Switch (config-l2nat)# outside from host 10.1.0.100 to 192.168.0.100
```

次に、5 つの外部アドレスから対応する内部アドレスに変換するように Instance1 という名前のインスタンスを設定する例を示します。10.10.10.1 は 192.168.142.1 に、10.10.10.2 は 192.168.142.1 のようにマッピングされます。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# outside from range 10.10.10.1 to 192.168.142.1 5
```

次に、外部サブネット上のすべてのアドレスから内部サブネットのアドレスに変換するように Instance1 という名前のインスタンスを設定する例を示します。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# outside from network 20.20.30.0 to 192.168.142.0 mask 255.255.255.0
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">inside from</a>                     | レイヤ 2 NAT を使用して内部アドレスを外部アドレスに変換します。                         |
| <a href="#">l2nat</a>                           | 選択したインターフェイスの 1 つまたはすべての VLAN にレイヤ 2 NAT インスタンスを適用します。      |
| <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                           |
| <a href="#">show l2nat interface</a>            | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。                |
| <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# pagp learn-method

EtherChannel ポートから受信した着信パケットの送信元アドレスを学習するには、インターフェイス コンフィギュレーション モードで **pagp learn-method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
pagp learn-method {aggregation-port | physical-port}
```

```
no pagp learn-method
```

## 構文の説明

|                         |                                       |
|-------------------------|---------------------------------------|
| <b>aggregation-port</b> | 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。          |
| <b>physical-port</b>    | EtherChannel 内の物理ポートで学習する アドレスを指定します。 |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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。

スイッチは、送信元アドレスを学習したものと同一 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。

学習方式は、リンクの両端で同一の設定にする必要があります。

コマンドライン インターフェイス (CLI) を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレスの学習だけです。スイッチ ハードウェアでは、**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは無効ですが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習だけをサポートするデバイスとの PAgP の相互運用にはこれらのコマンドが必要です。

スイッチへのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用してスイッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用して送信元 MAC アドレスに基づいた負荷分散方式を設定することを推奨します。この状況でだけ、**pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

## 例

次の例では、学習方式を設定し、EtherChannel 内の物理ポート上のアドレスを学習する方法を示します。

```
Switch(config-if)# pagp learn-method physical-port
```

## ■ pagp learn-method

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  |
|----------------------------|---|
| <b>pagp port-priority</b>  | 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。  |
| <b>show pagp</b>           | PAgP チャンネル グループ情報を表示します。  |
| <b>show running-config</b> | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# pagp port-priority

EtherChannel 経由のポート集約プロトコル (PAgP) のすべてのトラフィックが送信されるポートを選択するには、インターフェイス コンフィギュレーション モードで **pagp port-priority** 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働状態にできます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**pagp port-priority** *priority*

**no pagp port-priority**

## 構文の説明

*priority* プライオリティ番号は 0 ~ 255 です。

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

同じ EtherChannel 内で動作可能でメンバーシップを持つ物理ポートの中で最も高いプライオリティを持つポートが、PAgP 送信用として選択されます。

コマンドライン インターフェイス (CLI) を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレスの学習だけです。スイッチ ハードウェアでは、**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは無効ですが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習だけをサポートするデバイスとの PAgP の相互運用にはこれらのコマンドが必要です。

スイッチへのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用してスイッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用して送信元 MAC アドレスに基づいた負荷分散方式を設定することを推奨します。この状況でだけ、**pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

## 例

次の例では、ポート プライオリティを 200 に設定する方法を示します。

```
Switch(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp channel-group-number internal** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                              | 説明                           |
|-----------------------------------|------------------------------|
| <a href="#">pagp learn-method</a> | 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。 |

| コマンド                       | 説明  |
|----------------------------|---|
| <a href="#">show pagp</a>  | PAgP チャンネル グループ情報を表示します。  |
| <b>show running-config</b> | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# permit (ARP アクセス リスト コンフィギュレーション)

ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) バインディングとの一致に基づいて ARP パケットを許可するには、コンフィギュレーション モードで **permit** アドレス解決プロトコル (ARP) アクセスリスト 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アクセス コントロール エントリ (ACE) を削除するには、このコマンドの **no** 形式を使用します。

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

```
no permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}]} [log]
```

## 構文の説明

|                                   |  |
|-----------------------------------|--|
| <b>request</b>                    | (任意) ARP 要求の照合を要求します。 <b>request</b> 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。  |
| <b>ip</b>                         | 送信元 IP アドレスを指定します。   |
| <b>any</b>                        | IP または MAC アドレスを受け入れます。  |
| <b>host sender-ip</b>             | 指定された送信側 IP アドレスを受け入れます。   |
| <b>sender-ip sender-ip-mask</b>   | 指定された範囲の送信側 IP アドレスを受け入れます。  |
| <b>mac</b>                        | 送信元 MAC アドレスを指定します。  |
| <b>host sender-mac</b>            | 指定された送信側 MAC アドレスを受け入れます。  |
| <b>sender-mac sender-mac-mask</b> | 指定された範囲の送信側 MAC アドレスを受け入れます。   |
| <b>response ip</b>                | ARP 応答の IP アドレス値を定義します。  |
| <b>host target-ip</b>             | (任意) 指定されたターゲット IP アドレスを受け入れます。  |
| <b>target-ip target-ip-mask</b>   | (任意) 指定された範囲のターゲット IP アドレスを受け入れます。   |
| <b>mac</b>                        | ARP 応答の MAC アドレス値を指定します。   |
| <b>host target-mac</b>            | (任意) 指定されたターゲット MAC アドレスを受け入れます。   |
| <b>target-mac target-mac-mask</b> | (任意) 指定された範囲のターゲット MAC アドレスを受け入れます。  |
| <b>log</b>                        | (任意) ACE と一致するパケットを記録します。 <b>ip arp inspection vlan logging</b> グローバル コンフィギュレーション コマンドで <b>matchlog</b> 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。 |

## コマンドデフォルト

なし

## 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

## ■ permit (ARP アクセス リスト コンフィギュレーション)

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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
```

| 関連コマンド | コマンド  | 説明  |
|--------|---|---|
|        | <a href="#">arp access-list</a>                 | ARP アクセス コントロール リスト (ACL) を定義します。             |
|        | <a href="#">deny (ARP アクセス リスト コンフィギュレーション)</a> | 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。         |
|        | <a href="#">ip arp inspection filter vlan</a>   | 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。 |
|        | <a href="#">show access-lists</a>               | ARP アクセス リストに関する詳細を表示します。                     |

## permit (config-l2nat コンフィギュレーション)

ユニキャスト トラフィックだけ変換の対象となります。変換するよう設定されていないトラフィックの指定されたタイプを許可またはブロックするには、config-l2nat モードで **permit** コマンドを使用します。

変換するよう設定されていないトラフィックの指定されたタイプをドロップするには、このコマンドの **no** 形式を入力します。

```
permit { unmatched | multicast | igmp | all } [in|out]
```

```
no permit { unmatched | multicast | igmp | all } [in|out]
```



(注)

パススルー プロトコルには、SNMP、PROFINET、SIP (Voip)、Skinny、PTP、Telnet、FTP、SSH が含まれます。これらのプロトコルは、IP レイヤ上に追加の NAT 処理は必要ではありません。

### 構文の説明

|                  |  |
|------------------|--|
| <b>unmatched</b> | このレイヤ 2 NAT インスタンスの変換エントリに含まれないユニキャスト パケット。                                |
| <b>multicast</b> | マルチキャスト パケット。  |
| <b>igmp</b>      | IGMP パケット  |
| <b>all</b>       | すべての unmatched、multicast および IGMP パケット。                                    |
| <b>in</b>        | (任意) アップリンク経路で着信するパケット。このコマンドを両方向 (デフォルト設定) のトラフィックに適用するには、このパラメータを省略します。  |
| <b>out</b>       | (任意) アップリンク経路で出力されるパケット。このコマンドを両方向 (デフォルト設定) のトラフィックに適用するには、このパラメータを省略します。 |

### コマンド デフォルト

両方向のアップリンク経路でリストされたトラフィックのタイプすべてをドロップします

### コマンド モード

Config-l2nat configuration

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(2)EB | このコマンドが導入されました。 |

### 使用上のガイドライン

各レイヤ 2 NAT インスタンスに対するこれらの設定を行います。

### 例

次に、Instance1 という名前のインスタンスを設定し、アップリンク経路で着信するマルチキャスト トラフィックを許可する例を示します。

```
Switch(config)# l2nat instance Instance1
Switch(config-l2nat)# permit multicast in
```

## ■ permit (config-l2nat コンフィギュレーション)

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">l2nat</a>                           | 選択したインターフェイスの 1 つまたはすべての VLAN にレイヤ 2 NAT インスタンスを適用します。      |
| <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                           |
| <a href="#">show l2nat interface</a>            | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。                |
| <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# 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非 IP トラフィックの転送を許可するには、**permit** MAC access-list configuration モードを使用します。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 | lave-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 | lave-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

|  |   |
|--|---|
| <b>deny</b>                                  | すべての非 IP トラフィックを拒否するように指定します。   |
| <b>any</b>                                   | 送信元または宛先 MAC アドレスを拒否するように指定します。   |
| <b>host src-MAC-addr   src-MAC-addr mask</b> | 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。  |
| <b>host dst-MAC-addr   dst-MAC-addr mask</b> | 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。   |
| <b>type mask</b>                             | (任意) パケットのプロトコルを識別する Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号。 <ul style="list-style-type: none"> <li><b>type</b> には、0 ~ 65535 の 16 進数を指定できます。</li> <li><b>mask</b> は、一致をテストする前に Ethertype に適用される <i>don't care</i> ビットのマスクです。</li> </ul> |
| <b>aarp</b>                                  | (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。  |
| <b>amber</b>                                 | (任意) EtherType DEC-Amber を選択します。  |
| <b>cos cos</b>                               | (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。 <b>cos</b> 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。  |
| <b>dec-spanning</b>                          | (任意) EtherType Digital Equipment Corporation (DEC) スパニング ツリーを選択します。   |
| <b>decnet-iv</b>                             | (任意) EtherType DECnet Phase IV プロトコルを選択します。   |
| <b>diagnostic</b>                            | (任意) EtherType DEC-Diagnostic を選択します。   |
| <b>dsm</b>                                   | (任意) EtherType DEC-DSM を選択します。  |
| <b>etype-6000</b>                            | (任意) EtherType 0x6000 を選択します。   |
| <b>etype-8042</b>                            | (任意) EtherType 0x8042 を選択します。   |

## ■ permit (MAC アクセス リスト コンフィギュレーション)

|                              |   |
|------------------------------|---|
| <b>lat</b>                   | (任意) EtherType DEC-LAT を選択します。  |
| <b>lavr-sca</b>              | (任意) EtherType DEC-LAVC-SCA を選択します。   |
| <b>lsap lsap-number mask</b> | (任意) 802.2 カプセル化によるパケットの LSAP 番号 (0 ~ 65535) を指定して、パケットのプロトコルを識別します。<br><i>mask</i> は、一致をテストする前に LSAP 番号に適用される <i>don't care</i> ビットのマスクです。 |
| <b>mop-console</b>           | (任意) EtherType DEC-MOP Remote Console を選択します。   |
| <b>mop-dump</b>              | (任意) EtherType DEC-MOP Dump を選択します。   |
| <b>msdos</b>                 | (任意) EtherType DEC-MSDOS を選択します。  |
| <b>mumps</b>                 | (任意) EtherType DEC-MUMPS を選択します。  |
| <b>netbios</b>               | (任意) EtherType DEC-Network Basic Input/Output System (NETBIOS) を選択します。  |
| <b>vines-echo</b>            | (任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) Echo を選択します。   |
| <b>vines-ip</b>              | (任意) EtherType VINES IP を選択します。   |
| <b>xns-idp</b>               | (任意) EtherType Xerox Network Systems (XNS) プロトコルスイートを選択します。   |

## コマンド デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルトアクションは拒否です。

## コマンド モード

MAC アクセス リスト コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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* 変数を使用します。表 2-15 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 2-15 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  | Novell 名       |                  |
| arpa         | Ethernet II    | Ethertype 0x8137 |
| snap         | Ethernet-snap  | Ethertype 0x8137 |
| sap          | Ethernet 802.2 | LSAP 0xE0E0      |
| novell-ether | Ethernet 802.3 | LSAP 0xFFFF      |

**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。

アクセス コントロール エントリ (ACE) が ACL に追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

名前付き MAC 拡張アクセス リストの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

**例**

次の例では、あらゆる送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを許可する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは許可されます。

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

次の例では、名前付き MAC 拡張アクセス リストから許可条件を削除する方法を示します。

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、Ethertype 0x4321 のすべてのパケットを許可します。

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

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

**関連コマンド**

| コマンド                                   | 説明   |
|--|--|
| <b>deny (MAC アクセス リスト コンフィギュレーション)</b> | 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。        |
| <b>mac access-list extended</b>        | 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。 |
| <b>show access-lists</b>               | スイッチに設定されたアクセス コントロール リストを表示します。           |

# police

分類したトラフィックにポリサーを定義するには、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 **police** コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。既存のポリサーを削除するには、このコマンドの **no** 形式を使用します。

**police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]**

**no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]**

## 構文の説明

|  |   |
|--|---|
| <i>rate-bps</i>                            | ビット/秒 (b/s) の平均トラフィック伝送速度。指定できる範囲は 1000000 ~ 1000000000 です。   |
| <i>burst-byte</i>                          | 通常のバースト サイズ (バイト単位)。指定できる範囲は 8000 ~ 1000000 です。   |
| <b>exceed-action drop</b>                  | (任意) 指定された伝送速度を超えた場合は、スイッチがパケットをドロップするように指定します。   |
| <b>exceed-action policed-dscp-transmit</b> | (任意) 指定された伝送速度を超えた場合、スイッチがパケットの Diffserv コード ポイント (DSCP) をポリシング設定 DSCP マップに指定された値に変え、パケットを送信するように指定します。 |

## コマンド デフォルト

ポリサーは定義されません。

## コマンド モード

ポリシー マップ クラス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

階層ポリシー マップを設定する場合、セカンダリ インターフェイス レベルのポリシー マップで使用できるのは **police** ポリシー マップ コマンドだけです。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー (255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー) をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるという保証はありません。

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

ポリシングは、トークンバケットアルゴリズムを使用します。バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの *rate-bps* オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

**例**

次の例では、トラフィックがバースト サイズ 20 KB で平均伝送速度 1 Mb/s を超えた場合に、ポリサーがパケットをドロップするように設定する方法を示します。着信パケットの DSCP が信頼され、パケットは変更されません。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action drop
Switch(config-pmap-c)# exit
```

次の例では、DSCP 値をポリシング設定 DSCP マップに定義された値でマークダウンしてパケットを送信するポリサーを設定する方法を示します。

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

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

**関連コマンド**

| コマンド                            | 説明   |
|---------------------------------|--|
| <b>class</b>                    | 指定されたクラスマップ名のトラフィック分類一致条件 ( <b>police</b> 、 <b>set</b> 、および <b>trust</b> ポリシー マップ クラス コンフィギュレーション コマンドによる) を定義します。 |
| <b>mls qos map policed-dscp</b> | ポリシング設定 DSCP マップを DSCP の信頼できるポートに適用します。  |
| <b>policy-map</b>               | 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。  |
| <b>set</b>                      | パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。  |
| <b>show policy-map</b>          | Quality of Service (QoS) ポリシー マップを表示します。   |
| <b>trust</b>                    | <b>class</b> ポリシー マップ コンフィギュレーション コマンドまたは <b>class-map</b> グローバル コンフィギュレーション コマンドを使用して分類されたトラフィックの信頼状態を定義します。      |

# police aggregate

同じポリシー 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 **police aggregate** コマンドを使用します。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。

## コマンドデフォルト

集約ポリサーは定義されません。

## コマンドモード

ポリシー マップ クラス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるという保証はありません。

集約ポリサー パラメータを設定するには、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。集約ポリサーは同じポリシー マップ内の複数のクラスに適用されます。異なるポリシー マップにまたがって集約ポリサーを使用することはできません。

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

階層ポリシー マップで集約ポリサーを設定することはできません。

## 例

次の例では、集約ポリサー パラメータを定義する方法と、ポリシー マップ内の複数のクラスにそのポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

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

## 関連コマンド

| コマンド                                  | 説明                                       |
|---------------------------------------|--|
| <b>mls qos aggregate-policer</b>      | ポリシー マップ内の複数のクラスが共有できるポリサー パラメータを定義します。  |
| <b>show mls qos aggregate-policer</b> | Quality of Service (QoS) 集約ポリサー設定を表示します。 |

# policy-map

複数の物理ポートまたはスイッチ仮想インターフェイス (SVI) に適用し、ポリシーマップ コンフィギュレーション モードを開始できるポリシー マップを作成または変更するには、グローバル コンフィギュレーション モードで **policy-map** コマンドを使用します。既存のポリシー マップを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

## 構文の説明

*policy-map-name* ポリシー マップ名です。

## コマンドデフォルト

ポリシー マップは定義されません。

デフォルトの動作は、パケットが IP パケットの場合には Diffserv コード ポイント (DSCP) を 0 に設定し、パケットがタグ付きの場合には Class of Service (CoS) を 0 に設定します。ポリシングは実行されません。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**policy-map** コマンドを入力すると、ポリシー マップ コンフィギュレーション モードに入り、次のコンフィギュレーション コマンドが使用可能になります。

- **class** : 指定したクラス マップの分類一致基準を定義します。詳細については、「[class](#)」(P.2-83)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** : 定義済みポリシー マップを削除します。
- **rename** : 現在のポリシー マップの名前を変更します。

グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

一致基準がクラス マップに定義されているクラスのポリシーを設定する前に、**policy-map** コマンドを使用して作成、追加または変更するポリシー マップの名前を指定します。**policy-map** コマンドを入力した場合も、ポリシー マップ コンフィギュレーション モードがイネーブルになり、このモードでポリシー マップのクラス ポリシーを設定または変更することができます。

クラス ポリシーをポリシー マップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。クラスの一致基準を設定するには、**class-map** グローバル コンフィギュレーション コマンドおよび **match** クラス マップ コンフィギュレーション コマンドを使用します。物理ポート単位でパケット分類を定義します。

1つの入力ポートまたは SVI では、1つのポリシー マップだけがサポートされています。同じポリシー マップを複数の物理ポートまたは SVI に適用できます。

非階層ポリシー マップを物理ポートまたは SVI に適用できます。ただし、階層ポリシー マップを適用できるのは SVI だけです。

階層ポリシー マップには2つのレベルがあります。1つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。もう1つはインターフェイス レベルで、インターフェイス レベルのポリシー マップに指定されていて、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。

プライマリ VLAN レベル ポリシー マップでは、信頼状態の設定、あるいはパケットでの新しい DSCP または IP precedence 値の設定だけが可能です。セカンダリ インターフェイス レベル ポリシー マップでは、SVI に属する物理ポートの個々のポリサーの設定だけが可能です。

階層ポリシー マップを SVI に適用すると、インターフェイス レベル ポリシー マップを変更したり、階層ポリシー マップから削除したりすることはできません。階層ポリシー マップに、新しいインターフェイス レベル ポリシー マップを追加することもできません。このような変更を行いたい場合は、まず階層ポリシー マップを SVI から削除する必要があります。

階層ポリシー マップの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring QoS」の章の「Policing on SVIs」を参照してください。

## 例

次の例では、`policy1` という名前のポリシー マップを作成する方法を示します。入力ポートに適用した場合、`class1` で定義されたすべての着信トラフィックの照合を行い、IP DSCP を 10 に設定し、平均伝送速度 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイルを超過するトラフィックは、ポリシング設定 DSCP マップから受信した DSCP 値がマークされてから送信されます。

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

次の例では、ポリシー マップ `polycy2` に複数のクラスを設定する方法を示します。

```
Switch(config)# policy-map polycy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 100000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 100000 20000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp 0 (no policer)
Switch(config-pmap-c)# exit
```

次の例は、階層ポリシー マップを作成し、SVI に適用する方法を示しています。

```
Switch(config)# class-map cm-non-int
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-non-int-2
Switch(config-cmap)# match access-group 102
Switch(config-cmap)# exit
Switch(config)# class-map cm-test-int
Switch(config-cmap)# match input-interface gigabitethernet1/2 - gigabitethernet1/2
Switch(config-cmap)# exit
Switch(config)# policy-map pm-test-int
Switch(config-pmap)# class cm-test-int
Switch(config-pmap-c)# police 18000000 8000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map pm-test-pm-2
Switch(config-pmap)# class cm-non-int
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap)# class cm-non-int-2
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap-c)# end
Switch(config-cmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input pm-test-pm-2
```

次の例では、policymap2 を削除する方法を示します。

```
Switch(config)# no policy-map policymap2
```

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

## 関連コマンド

| コマンド                     | 説明  |
|--------------------------|---|
| <b>class</b>             | 指定のクラスマップ名のトラフィック分類の一致基準を定義します (police、set、および trust ポリシー マップ クラス コンフィギュレーション コマンドを使用)。 |
| <b>class-map</b>         | 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。   |
| <b>service-policy</b>    | ポートにポリシー マップを適用します。   |
| <b>show mls qos vlan</b> | SVI に適用されている Quality of Service (QoS) ポリシー マップを表示します。                                   |
| <b>show policy-map</b>   | 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、グローバル コンフィギュレーション モードで **port-channel load-balance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}
```

```
no port-channel load-balance
```

## 構文の説明

|                    |  |
|--------------------|--|
| <b>dst-ip</b>      | 宛先ホストの IP アドレスに基づいて配信を設定します。   |
| <b>dst-mac</b>     | 宛先ホストの MAC アドレスに基づいて配信を設定します。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。 |
| <b>src-dst-ip</b>  | 送信元および宛先ホストの IP アドレスに基づいて配信を設定します。   |
| <b>src-dst-mac</b> | 送信元および宛先ホストの MAC アドレスに基づいて配信を設定します。  |
| <b>src-ip</b>      | 送信元ホストの IP アドレスに基づいて配信を設定します。  |
| <b>src-mac</b>     | 送信元 MAC アドレスに基づいて配信を設定します。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。  |

## コマンド デフォルト

デフォルトは、**src-mac** です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 (EtherChannel の設定)」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  |
|--|---|
| <a href="#">interface port-channel</a> | 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。   |
| <a href="#">show etherchannel</a>      | チャンネルの EtherChannel 情報を表示します。   |
| <a href="#">show running-config</a>    | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# power inline

Power over Ethernet (PoE) と (PoE+) ポートで電源管理モードを設定するには、**power inline** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
power inline {auto [max max-wattage] | never | consumption | static [max max-wattage]}
```

```
no power inline {auto | never | consumption| static}
```

## 構文の説明

|                        |  |
|------------------------|--|
| <b>auto</b>            | 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。   |
| <b>max max-wattage</b> | (任意) ポートに供給される電力を制限します。電源デバイスに基づいて Cisco IE3000 スイッチでの範囲は 4000 ~ 30000 ミリワットです。値を指定しない場合は、最大電力が供給されます。 |
| <b>never</b>           | 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。  |
| <b>consumption</b>     | (任意) PoE ポートに接続した装置に割り当てられた電力を指定します。   |
| <b>static</b>          | 受電装置の検出をイネーブルにします。スイッチが受電装置を検出する前に、ポートへの電力を事前に割り当てます (確保します)。  |

## デフォルト

デフォルトの設定は **auto** (イネーブル) です。

最大ワット数は、PoE スイッチでは 15400 ミリワット、PoE+ スイッチでは 30000 ミリワットです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース       | 変更内容            |
|------------|-----------------|
| 15.0(2)EY1 | 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 対応ポートと拡張モジュールが搭載されたスイッチでのみサポートされます。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 fastEthernet 2/1
Switch(config-if) # power inline auto
                        ^
% Invalid input detected at '^' marker.
```

すべての PoE 対応スイッチ ポートは、IEEE 802.3 af に準拠しています。PoE+ および PoE 対応ポートを備えたスイッチは IEEE 802.3 at に準拠しています。

**max max-wattage** オプションを使用して、受電デバイス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、受電デバイス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、グローバル電力バジェットに送られます。



(注)

**power inline max max-wattage** コマンドが PoE スイッチで 15400 ミリワット未満に、または PoE+ スイッチで 30000 ミリワット未満に設定されている場合、スイッチはどの Class 0 または Class 3 デバイスにも電源を供給しません。

スイッチが受電デバイスへの電力供給を拒否する場合（受電デバイスが CDP メッセージを通じて制限を超えた電力を要求する場合、または IEEE クラスの最大値が最大ワット数を超えている場合）、PoE ポートは **power-deny** ステートになります。スイッチはシステム メッセージを生成し、**show power inline** ユーザ EXEC コマンド出力の Oper カラムに **power-deny** が表示されます。

ポートに高いプライオリティを与えるには、**power inline static max max-wattage** コマンドを使用します。スイッチは、**auto** モードに設定されたポートに電力を割り当てる前に、**static** モードに設定されたポートに PoE を割り当てます。スイッチは、装置検出より優先的に設定されている場合に、スタティック ポートの電力を確保します。接続された装置がない場合は、ポートがシャットダウン状態か否かに関係なく、スタティック ポートの電力が確保されます。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電デバイスからの 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られているので、最大ワット数以下の電力を使用する受電デバイスは、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、受電デバイスの 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デバイス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、受電デバイスがシャットダウンします。

ポートが **static** モードの場合にスイッチが電力を事前割り当てできない場合（たとえば、電力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（これが受電デバイスであるかどうかに関係なく）接続された装置の所要電力を判別するのに必要な、設定された速度とデュプレックス設定を使用して自動的にをネゴシエートします。電力要件が判別された後、スイッチはインターフェイスをリセットすることなく、設定された速度とデュプレックス設定を使用してインターフェイスをハードコードします。

**power inline never** コマンドを使用してポートを設定する場合、ポートは設定された速度とデュプレックス設定に戻ります。

ポートにシスコ製の受電デバイスが接続されている場合は、**power inline never** コマンドでポートを設定しないでください。ポートで不正なリンクアップが生じ、**errdisable** ステートになる可能性があります。

**例**

次の例では、受電デバイス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 fastEthernet 2/1
Switch(config-if)# power inline auto
```

次の例では、Class 1 または Class 2 の受電デバイスを受け入れるように PoE ポートを設定する方法を示します。

```
Switch(config)# interface fastEthernet 2/1
Switch(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、PoE ポートへの電力供給を停止する方法を示します。

```
Switch(config)# interface fastEthernet 2/1
Switch(config-if)# power inline never
```

設定を確認するには、**show power inline** ユーザ EXEC コマンドを入力します。

**関連コマンド**

| コマンド   | 説明  |
|--|---|
| <b>logging event<br/>power-inline-status</b> | PoE イベントのロギングをイネーブルにします。                      |
| <b>show controllers<br/>power inline</b>     | 指定した PoE コントローラのレジスタ値を表示します。                  |
| <b>show power inline</b>                     | 指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。 |

# power inline consumption

各受電デバイスが使用するワット数を指定することにより、デバイスの IEEE 分類で指定された電力量を上書きするには、**power inline consumption** グローバルまたはインターフェイス コンフィギュレーション コマンドを使用します。デフォルトの電力設定に戻すには、このコマンドの **no** 形式を使用します。

**power inline consumption default wattage**

**no power inline consumption default**

## 構文の説明

*wattage* スイッチがポート用に確保する電力。指定できる範囲は、PoE スイッチでは 4000 ~ 15400 ミリワット、PoE+ スイッチでは 4000 ~ 30000 ミリワットです。

## デフォルト

デフォルト電力は各 Power over Ethernet (PoE) ポートで 15400 ミリワット、各 PoE+ ポートでは 30000 ミリワットです。



(注)

**default** キーワードは、グローバル コンフィギュレーション コマンドでだけ表示されます。

## コマンドモード

グローバル コンフィギュレーション  
インターフェイス コンフィギュレーション

## コマンド履歴

| リリース       | 変更内容            |
|------------|-----------------|
| 15.0(2)EY1 | このコマンドが追加されました。 |

## 使用上のガイドライン

シスコの受電デバイスが PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol (CDP) を使用して実際に装置が消費する電力量を決定して、それに応じて電力バジェットを調整します。この機能は、IEEE サードパーティの受電デバイスには適用されません。この装置の場合、スイッチが電力要求を許可したときに、受電装置の IEEE 分類に応じて電力バジェットを調整します。受電デバイスが Class 0 (クラス ステータスは不明) または Class 3 である場合、実際に必要な電力量に関係なく、スイッチは装置用に 15400 ミリワットの電力を確保します。受電デバイスが実際の電力消費量よりも高いクラスであるか、または電力分類 (デフォルトで Class 0) をサポートしない場合、スイッチは IEEE クラス情報を使用してグローバル電力バジェットを追跡するので、少しの装置にしか電力を供給しません。

**power inline consumption wattage** コンフィギュレーション コマンドを使用することで、IEEE 分類で指定されたデフォルトの電力要件を無効にできます。IEEE 分類で指定された電力と実際に装置が必要とする電力の差は、追加の装置が使用するためグローバル電力バジェットに入れられます。したがって、スイッチの電力バジェットを拡張してもっと効率的に使用できます。



注意

慎重にスイッチの電力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: Misconfiguring the 'power inline consumption/allocation' command may cause damage to the switch and void your warranty. Take precaution not to oversubscribe the power supply. Refer to documentation.



(注)

手動で電力バジェットを設定する場合、スイッチと受電デバイス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 電力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 (インターフェイス特性の設定)」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 ミリワットの電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# power inline consumption default 5000
%CAUTION: Misconfiguring the 'power inline consumption/allocation' command may cause
damage to the switch and void your warranty. Take precaution not to oversubscribe the
power supply. Refer to documentation.
```

次の例では、インターフェイス コンフィギュレーション コマンドを使用して、特定の PoE ポートに接続された受電デバイスに 12000 ミリワットの電力を確保するようスイッチを設定する方法を示します。

```
Switch(config) # interface fastEthernet 1/1
Switch(config-if)# power inline consumption 12000
%CAUTION: Misconfiguring the 'power inline consumption/allocation' command may cause
damage to the switch and void your warranty. Take precaution not to oversubscribe the
power supply. Refer to documentation.
```

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

関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">logging event power-inline-status</a> | PoE イベントのログギングをイネーブルにします。                     |
| <a href="#">power inline</a>                      | PoE ポート上で電力管理モードを設定します。                       |
| <a href="#">show power inline</a>                 | 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 wattage

PoE 装置に使用する電源装置の合計電力ワット数の PoE 単位の電力バジェットを変更するには、**power inline wattage** グローバル コンフィギュレーション コマンドを使用します。デフォルトの電力バジェット設定に戻すには、このコマンドの **no** 形式を使用します。

**power inline wattage**

**no power inline wattage**

## 構文の説明

**wattage** 使用可能な合計 PoE ワットの PoE 単位の電力バジェットを変更します。  
このコマンドは、ユニットに設置されている電源デバイスをリセットします。ミリワット範囲は 4000～130000 ミリワットです。PoE 単位で使用されている電源の評価に基づき、電源のワット数を設定できます。

## デフォルト

シスコ標準の小さいブロックの電源を使用して PoE 装置に電力を供給している場合は、デフォルトの電力バジェットは 65 ワットです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(2)EA | このコマンドが追加されました。 |

## 使用上のガイドライン

スイッチの電力バジェットを変更するには、**power inline wattage** コマンドを使用できます。このコマンドは合計電力バジェットを変更し、新しい電力バジェットに合わせてスイッチに設置されている電源デバイスをリセットします。設定した新しい電力バジェットはグローバル設定で保存されます。

より高いまたは低い電源ワット数に移行するには、各 PoE ポートに適切な電源が割り当てられるようにスイッチの合計電力バジェットを増減してください。デフォルトでは、スイッチはシスコ標準の小さいブロック電源を想定して、65 ワットの電力バジェットを使用します。

このコマンドの使用には注意メッセージが表示されます。

**%CAUTION:** Misconfiguring the 'power inline' wattage command may cause damage to the switch. Take precaution not to oversubscribe the power supply. Command will result in reset of the PD(s)connected. Refer to documentation.

電力制限の超過を避けるには、各ケースに応じた次の手順に従います。

ケース 1：合計電力バジェットを上げる。

- ステップ 1** 電源を変更します。
- ステップ 2** CLI を使用して合計電力バジェットを変更します。

ケース 2：合計電力バジェットを下げる。

- ステップ 1** CLI を使用して合計電力バジェットを変更します。

**ステップ 2** 電源を変更します。**例**

次に、合計 PoE ワット数の電源を変更する例を示します。

```
switch(config)# power inline ?
  consumption  Inline device power consumption
  wattage      Modify power supply total PoE watts available
switch(config)# power inline wattage ?
max maximum wattage as per input power supply rating
switch(config)# power inline wattage max ?
<4-130> watts
<cr>
switch(config)# power inline wattage max 50
```

**関連コマンド**

| コマンド  | 説明  |
|---|---|
| <a href="#">logging event power-inline-status</a> | PoE イベントのロギングをイネーブルにします。                      |
| <a href="#">power inline</a>                      | PoE ポート上で電力管理モードを設定します。                       |
| <a href="#">power inline consumption</a>          | スイッチがポート用に確保する電力を指定します。                       |
| <a href="#">show power inline</a>                 | 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。 |
| <a href="#">show controllers power inline</a>     | 指定した PoE コントローラのレジスタ値を表示します。                  |

# power-supply dual

デュアル電源モードを設定するには、グローバル コンフィギュレーション モードで **power-supply dual** コマンドを使用します。デフォルトのシングル電源モードに戻すには、このコマンドの **no** 形式を使用します。

**power-supply dual**

**no power-supply dual**

## 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

デフォルトでは、システムはシングル電源モードで稼働しています。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

スイッチには、DC 電源入力 が 2 つ搭載されています。スイッチが 2 つめの DC 入力に接続されデュアル電源モードに変更された状態で、プライマリ電源で障害が発生すると、2 つめの電源からスイッチに電力が供給されます。

スイッチがデュアル電源モードの場合、**alarm facility power-supply** グローバル コンフィギュレーション コマンドを使用してアラーム オプションを設定できます。プライマリ電源の欠落または障害をモニタするには、**show facility-alarm status** ユーザ EXEC コマンドを使用します。

## 例

次の例では、スイッチをデュアル電源モードに設定する方法を示します。

```
Switch(config)# power-supply dual
```

## 関連コマンド

| コマンド  | 説明                                     |
|---|--|
| <a href="#">alarm facility power-supply</a> | スイッチで電源の欠落または障害をモニタし、アラーム オプションを設定します。 |
| <a href="#">show alarm settings</a>         | 環境アラーム設定およびオプションが表示されます。               |

# priority-queue

ポート上で出力緊急キューをイネーブルにするには、インターフェイス コンフィギュレーション モードで **priority-queue** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**priority-queue out**

**no priority-queue out**

## 構文の説明

**out** 出力緊急キューをイネーブルにします。

## コマンド デフォルト

出力緊急キューは、ディセーブルです。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**priority-queue out** コマンドを設定する場合、シェイプド ラウンドロビン (SRR) に参加するキューが 1 つ少ないため、SRR の重み比が影響を受けます。これは、**srr-queue bandwidth shape** 内の **weight1** または **srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドが無視されることを意味します (比率計算に使用されません)。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して **shaped** モードは **shared** モードを無効にし、SRR はこのキューに **shaped** モードでサービスを提供します。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングされた重みが設定されていない場合は、SRR はキューに対して **shared** モードでサービスを提供します。

## 例

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
```

次の例では、SRR のシェーピングおよび共有された重みが設定された後、出力緊急キューをディセーブルにする方法を示します。シェーピングモードは、共有モードを無効にします。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

**show mls qos interface interface-id queueing** または **show running-config** 特権 EXEC コマンドを入力すれば、設定を確認することができます。

#### 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">show mls qos interface queueing</a> | キューイング方法 (SRR、プライオリティ キューイング)、キューに相応する重み、および Class of Service (CoS) から出力キューへのマップを表示します。 |
| <a href="#">srr-queue bandwidth shape</a>       | シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。                           |
| <a href="#">srr-queue bandwidth share</a>       | 共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。                                   |

# profinet

PROFINET の入出力 (IO) デバイスとしてスイッチを設定するには、グローバル コンフィギュレーション モードで **profinet** コマンドを使用します。PROFINET 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。

```
profinet [id line] vlan vlan id
```

```
no profinet [id line] vlan vlan id
```

## 構文の説明

|                     |  |
|---------------------|--|
| <b>id line</b>      | (任意) Cisco IOS ソフトウェアを使用して、PROFINET デバイス名を設定します。<br><br>最大長は 240 文字です。使用可能な特殊文字はピリオド (.) とハイフン (-) のみです。これらの文字は ID 文字列内の特定のオプションでのみ使用可能です。PROFINET ID では、文字列内で複数のラベルを使用できます。各ラベルに使用できる文字数は 1 ~ 63 文字です。複数のラベルはピリオド (.) で区切る必要があります。文字列内の末尾文字はゼロ (0) にしないでください。<br><br>PROFINET ID の設定の詳細については、PROFINET の仕様、文書番号 TC2-06-0007a、ファイル名 PN-AL-protocol_2722_V22_Oct07 を参照してください ( <a href="#">PROFIBUS</a> から入手できます)。 |
| <b>vlan vlan id</b> | (任意) PROFINET で使用する VLAN を指定します。VLAN ID の範囲は 1 ~ 4094 です。  |

## コマンドデフォルト

PROFINET が設定済みです。  
PROFINET ID が設定されていません。  
デフォルト VLAN は 1 です。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

通常、PROFINET 設定は、シスコ コマンドライン インターフェイス (CLI) を使用せずに設定します。PROFINET 管理ソフトウェアでは、レイヤ 2 Discovery and Configuration Protocol (DCP) を使用してスイッチに IP アドレスと PROFINET ID を設定し、デフォルト VLAN 番号を変更します。

## 例

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

```
Switch# configure terminal
Switch(config)# profinet
```

## 関連コマンド

| コマンド                                 | 説明  |
|--------------------------------------|---|
| <code>debug profinet alarm</code>    | PROFINET アラームのデバッグをイネーブルにします。   |
| <code>debug profinet cyclic</code>   | PROFINET 巡回パケットの送受信に関連するファンクション コールを表示します。  |
| <code>debug profinet error</code>    | PROFINET セッション エラーのデバッグをイネーブルにします。  |
| <code>debug profinet packet</code>   | PROFINET パケットのデバッグをイネーブルにします。   |
| <code>debug profinet platform</code> | Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにします。  |
| <code>debug profinet topology</code> | 受信した PROFINET トポロジ パケットを表示します。  |
| <code>debug profinet trace</code>    | トレースした一連のデバッグ出力ログを表示します。  |
| <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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <code>show profinet</code>           | スイッチの PROFINET セッションの詳細を表示します。  |

# psp

プロトコル パケットがスイッチに送信される速度を制御するには、グローバル コンフィギュレーション モードで **psp** コマンドを使用して、パケット フロー レートの上限しきい値を指定します。プロトコル ストーム プロテクション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。

```
psp {arp | dhcp | igmp} pps value
```

```
no psp {arp | dhcp | igmp}
```

## 構文の説明

|                  |  |
|------------------|--|
| <b>arp</b>       | ARP および ARP スヌーピングのプロトコル パケット フロー レートを設定します。   |
| <b>dhcp</b>      | DHCP および DHCP スヌーピングのプロトコル パケット フロー レートを設定します。                                       |
| <b>igmp</b>      | IGMP および IGMP スヌーピングのプロトコル パケット フロー レートを設定します。                                       |
| <b>pps value</b> | 秒あたりのパケット数のしきい値を指定します。トラフィックがこの値を超えると、プロトコル ストーム プロテクションが適用されます。範囲は毎秒 5 ~ 50 パケットです。 |

## コマンド デフォルト

プロトコル ストーム プロテクションはデフォルトでディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース       | 変更内容            |
|------------|-----------------|
| 15.0(58)SE | このコマンドが導入されました。 |

## 使用上のガイドライン

サポートされるプロトコルは、アドレス解決プロトコル (ARP)、ARP スヌーピング、ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) v4、DHCP スヌーピング、インターネット グループ管理プロトコル (IGMP)、および IGMP スヌーピングです。

**errdisable** 検出プロトコル ストーム プロテクションを設定するには、**errdisable detect cause psp** グローバル コンフィギュレーション コマンドを使用します。

プロトコル ストーム プロテクションが設定されている場合、ドロップされたパケットの数がカウンタに記録されます。特定のプロトコルのドロップされたパケットの数を表示するには、**show psp statistics {arp | dhcp | igmp}** 特権 EXEC コマンドを使用します。すべてのプロトコルのドロップされたパケットの数を表示するには、**show psp statistics all** コマンドを使用します。プロトコルのカウンタをクリアするには、**clear psp counter [arp | dhcp | igmp]** コマンドを使用します。

## 関連コマンド

| コマンド                               | 説明  |
|------------------------------------|---|
| <b>clear psp counter</b>           | ドロップされたパケットのカウンタをクリアします。                              |
| <b>errdisable detect cause psp</b> | プロトコル ストーム プロテクションの <b>errdisable</b> 検出機能をイネーブルにします。 |

| コマンド                             | 説明                           |
|----------------------------------|------------------------------|
| <code>show psp config</code>     | プロトコル ストーム プロテクションの設定を表示します。 |
| <code>show psp statistics</code> | ドロップされたパケットの数を表示します。         |

## ptp (グローバル コンフィギュレーション)

高精度時間プロトコル (PTP) のクロック プロパティを設定するには、グローバル コンフィギュレーション モードで **ptp** コマンドを使用します。デフォルトのエンドツーエンドの透過的なクロック モードに戻すには、このコマンドの **no** 形式を使用します。

```
ptp {mode {boundary | e2transparent | forward} | priority1 value | priority2 value}
```

```
no ptp {mode | priority1 | priority2}
```

### 構文の説明

|                        |   |
|------------------------|---|
| <b>mode</b>            | クロック モードを設定します。   |
| <b>boundary</b>        | すべての接続デバイスに対するグラントマスター クロックと親クロックとして機能します。最も正確なマスター クロックの選択に参加するスイッチをイネーブルにします。<br><br>このモードは、過負荷または重負荷の状態により大きな遅延ジッタが生じるときに使用します。            |
| <b>e2transparent</b>   | すべてのスイッチ ポートをマスター クロックと同期します。これがデフォルトのクロック モードです。   |
| <b>forward</b>         | 受信 PTP パケットが通常のマルチキャスト トラフィックとしてスイッチをパススルーすることを許可します  |
| <b>priority1 value</b> | 最も正確なマスター クロックを選択するために、デフォルトの条件 (クロック品質、クロック クラスなど) を上書きします。低い値が優先されます。有効な範囲は 0 ~ 255 です。デフォルトは 128 です。                                       |
| <b>priority2 value</b> | 2 つのスイッチがデフォルトの条件に一致する場合に、一方が選択されるようにします。たとえば、 <b>priority2</b> 値を使用して、特定のスイッチが他の同等のスイッチよりも優先されるようにすることができます。有効な範囲は 0 ~ 255 です。デフォルトは 128 です。 |

### コマンド デフォルト

デフォルト モードはエンドツーエンドのトランスペアレント クロック モードです。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

クロック同期によってスイッチや他のネットワーク デバイスで同じ時間に基づいてイベントおよびタイムスタンプが使用されます。最初の同期のあと、スイッチと接続済み装置は、タイミング メッセージを交換して、クロックのオフセットとネットワークの遅延による時間の歪みを修正します。

**boundary** クロック モードが選択されると、スイッチはより正確なクロックが選ばれなければマスター クロックになることがあります。

**e2transparent** のクロック モードを選択した場合、スイッチはマスター クロックの選択に参加せず、マスター クロックと同期しません。このモードでは、境界モードよりもジッタとエラーの蓄積が少なくなります。

## ■ ptp (グローバル コンフィギュレーション)

クロック選択基準が等しい場合 (**priority2** クロックを含め) クロック ID (スイッチ MAC アドレス) が優先順位を決定します。

ネットワーク マスター クロックの選択は継続して実行されます。デバイスがネットワークに追加されると、デバイスは自身とクロック パラメータをアナウンスします。新しいクロックが既存のクロックより正確であれば、それがマスターとなり、他のクロックはこのクロックと同期します。

**ptp priority1** および **ptp priority2** コマンドは、スイッチが境界モードの場合にのみ使用できます。

スイッチが PTP フォワード モードの場合、**show ptp clock** または **show ptp port** 特権 EXEC コマンドを入力すると、情報が使用できないことを示すエラー メッセージが表示されます。

スイッチが PTP フォワード モードの場合、PTP コンフィギュレーション モードだけを変更できます。スイッチがフォワード モードの場合、PTP ポート プロパティを設定できません。

## 例

次の例では、クロックをエンドツーエンド トランスペアレント モードに設定する方法を示します。

```
Switch(config)# ptp mode e2etransparent
```

次の例では、ローカル クロック **priority1** 値を 55 に設定する方法を示します。

```
Switch(config)# ptp priority1 55
```

## 関連コマンド

| コマンド                              | 説明  |
|-----------------------------------|---|
| <b>ptp (インターフェイス コンフィギュレーション)</b> | インターフェイス PTP クロック プロパティを設定します。                  |
| <b>show ptp</b>                   | グローバル プロパティおよびポートのプロパティを含むすべての PTP プロパティを表示します。 |
| <b>debug ptp</b>                  | PTP アクティビティのデバッグをイネーブルにします。                     |

## ptp (インターフェイス コンフィギュレーション)

ポートの高精度時間プロトコル (PTP) タイミング設定を指定するには、インターフェイス コンフィギュレーション モードで **ptp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ptp {announce {interval value | timeout value} | delay-req interval value | enable | sync {interval value | limit value}}
```

```
no ptp {announce {interval value | timeout value} | delay-req interval value | enable | sync {interval value | limit value}}
```

### 構文の説明

|                                 |  |
|---------------------------------|--|
| <b>announce interval value</b>  | アナウンス メッセージの送信ログ平均間隔を設定します。指定できる範囲は 0 ~ 4 です。デフォルトは 1 (2 秒) です。                              |
| <b>announce timeout value</b>   | タイムアウト メッセージをアナウンスする時間を設定します。欠落メッセージの範囲は 2 ~ 10 メッセージです。欠落メッセージのデフォルトは 3 メッセージです。            |
| <b>delay-req interval value</b> | 遅延要求メッセージの送信ログ平均間隔を設定します。範囲は .5 ~ 64 秒です。デフォルトは 5 (32 秒) です。                                 |
| <b>enable</b>                   | ポート上で PTP をイネーブルにします。  |
| <b>sync interval value</b>      | 同期メッセージの送信ログ平均間隔を設定します。範囲は .5 ~ 2 秒です。デフォルト値は 1 秒です。   |
| <b>sync limit value</b>         | クロック同期が失敗するまでのマスター クロックの最大オフセット値を設定します。指定できる範囲は 50 ~ 500000000 ナノ秒です。デフォルトは 500000000 ナノ秒です。 |

### コマンド デフォルト

PTP はイネーブルです。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

**ptp announce interval**、**ptp syn interval**、**ptp follow-up**、**ptp delay-response** コマンドは、ポートでマスター ステートが開始された場合にのみ送信されます。

タイミング設定は、スイッチが境界モードの場合にのみ使用できます。

### 例

次の例では、Gigabit Ethernet ポート 1 でアナウンス メッセージ送信間隔の値を 3 に設定する方法を示します。

```
Switch(config)# interface g1/1
Switch(config-if)# ptp announce interval 3
```

## ■ ptp (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  |
|--------|--------------------------------------|---|
|        | <code>ptp (グローバル コンフィギュレーション)</code> | グローバル PTP クロック プロパティを設定します。                     |
|        | <code>debug ptp</code>               | PTP アクティビティのデバッグをイネーブルにします。                     |
|        | <code>show ptp</code>                | グローバル プロパティおよびポートのプロパティを含むすべての PTP プロパティを表示します。 |

# queue-set

キューセットにポートをマッピングするには、インターフェイス コンフィギュレーション モードで **queue-set** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
queue-set qset-id
```

```
no queue-set qset-id
```

## 構文の説明

|                |   |
|----------------|---|
| <i>qset-id</i> | キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ~ 2 です。 |
|----------------|---|

## コマンドデフォルト

キューセット ID は 1 です。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# queue-set 2
```

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

## 関連コマンド

| コマンド   | 説明  |
|--|---|
| <a href="#">mls qos queue-set output buffers</a>   | バッファをキューセットに割り当てます。   |
| <a href="#">mls qos queue-set output threshold</a> | Weighted Tail-Drop (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当てを設定します。 |
| <a href="#">show mls qos interface buffers</a>     | Quality of Service (QoS) 情報を表示します。  |

# radius-server dead-criteria

RADIUS サーバが使用不可またはデット状態であることを判別する条件を設定するには、グローバル コンフィギュレーション モードで **radius-server dead-criteria** コマンドを使用します。デフォルト設定に戻すには、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取得するのをスイッチが必要としない時間 (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しない回数を指定します。範囲は 1 ~ 100 です。

## コマンド デフォルト

スイッチは、10 ~ 60 秒の *seconds* 値を動的に決定します。

スイッチは、10 ~ 100 の *tries* 値を動的に決定します。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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  |
|--------|--|---|
|        | <b>dot1x critical</b> (グローバル コンフィギュレーション)      | アクセス不能な認証バイパス機能のパラメータを設定します。  |
|        | <b>dot1x critical</b> (インターフェイス コンフィギュレーション)   | アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが <b>critical-authentication</b> 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。                |
|        | <b>radius-server retransmit</b> <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 Software Command Reference, Release 15.0』を参照してください。        |
|        | <b>radius-server timeout</b> <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 Software Command Reference, Release 15.0』を参照してください。 |
|        | <b>show running-config</b>                     | 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 Software Command Reference, Release 15.0』を参照してください。                                       |

# radius-server host

RADIUS アカウンティングおよび認証を含めた RADIUS サーバパラメータを設定するには、グローバル コンフィギュレーション モードで **radius-server host** コマンドを使用します。デフォルト設定に戻すには、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。  |
| <b>acct-port</b> <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。  |
| <b>auth-port</b> <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。   |
| <b>test username</b> <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。   |
| <b>idle-time</b> <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。範囲は 1 ~ 35791 分です。   |
| <b>ignore-acct-port</b>          | (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。  |
| <b>ignore-auth-port</b>          | (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。  |
| <b>key</b> <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。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト スtring でなければなりません。必ずこのコマンドの最終項目として <b>key</b> を設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 <b>key</b> にスペースが含まれる場合は、引用符が <b>key</b> の一部でない限り、 <b>key</b> を引用符で囲まないでください。 |

## コマンド デフォルト

RADIUS アカウンティング サーバの UDP ポートは 1646 です。

RADIUS 認証サーバの UDP ポートは 1645 です。

自動サーバテストはディセーブルです。

アイドル時間は 60 分 (1 時間) です。

自動テストがイネーブルの場合、UDP ポートのアカウンティングおよび認証時にテストが実行されます。

認証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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 ストリングを設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.2 acct-port 800 auth-port 900 test username
aaafail idle-time 75 key abc123
```

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

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <b>dot1x critical</b> (グローバル コンフィギュレーション)               | アクセス不能な認証バイパス機能のパラメータを設定します。  |
| <b>dot1x critical</b> (インターフェイス コンフィギュレーション)            | アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが <b>critical-authentication</b> 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。                      |
| <b>radius-server key {0 string   7 string   string}</b> | ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show running-config</b>                              | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。                                    |

# rcommand

Telnet セッションを開始し、クラスタ コマンド スイッチからクラスタ メンバ スイッチのコマンドを実行するには、クラスタ コマンド スイッチでユーザ EXEC モードの **rcommand** コマンドを使用します。セッションを終了するには、**exit** コマンドを入力します。

**rcommand** {*n* | **commander** | **mac-address hw-addr**}

## 構文の説明

|                            |  |
|----------------------------|--|
| <i>n</i>                   | クラスタ メンバを識別する番号。指定できる範囲は 0 ~ 15 です。          |
| <b>commander</b>           | クラスタ メンバ スイッチからクラスタ コマンド スイッチへアクセスできるようにします。 |
| <b>mac-address hw-addr</b> | クラスタ メンバ スイッチの MAC アドレスを指定します。               |

## コマンド デフォルト

なし

## コマンド モード

ユーザ EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でだけ使用できます。

スイッチがクラスタ コマンド スイッチで、クラスタ メンバ スイッチ *n* が存在していない場合、エラーメッセージが表示されます。スイッチ番号を得るには、クラスタ コマンド スイッチで **show cluster members** 特権 EXEC コマンドを入力します。

このコマンドを使用してクラスタ コマンド スイッチ プロンプトからクラスタ メンバ スイッチにアクセスしたり、メンバ スイッチ プロンプトからクラスタ コマンド スイッチにアクセスしたりすることができます。

Catalyst 2900 XL、Catalyst 3500 XL、Catalyst 2950、Catalyst 2960、Catalyst 2970、Catalyst 3550、Catalyst 3560、および Catalyst 3750 スイッチの場合、Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバ スイッチ コマンドライン インターフェイス (CLI) にアクセスします。たとえば、このコマンドをクラスタ コマンド スイッチからユーザ レベルで入力した場合、メンバ スイッチはユーザ レベルでアクセスされます。このコマンドをクラスタ コマンド スイッチからイネーブル レベルで使用した場合、コマンドはイネーブル レベルでリモート デバイスにアクセスします。権限レベルよりも低い中間イネーブル レベルを使用した場合、クラスタ メンバ スイッチはユーザ レベルとなります。

Standard Edition ソフトウェアが稼働している Catalyst 1900 および Catalyst 2820 スイッチの場合、クラスタ コマンド スイッチの権限レベルが 15 であれば、Telnet セッションはメニュー コンソール (メニュー方式インターフェイス) にアクセスします。クラスタ コマンド スイッチの権限レベルが 1 であれば、パスワードの入力を要求するプロンプトが表示され、入力後にメニュー コンソールにアクセスできます。クラスタ コマンド スイッチの権限レベルは、Standard Edition ソフトウェアが稼働しているクラスタ メンバ スイッチに次のようにマッピングします。

- クラスタ コマンド スイッチの権限レベルが 1 ~ 14 である場合、クラスタ メンバ スイッチへのアクセスは権限レベル 1 で行われます。
- クラスタ コマンド スイッチの権限レベルが 15 である場合、クラスタ メンバ スイッチへのアクセスは権限レベル 15 で行われます。

Catalyst 1900 および Catalyst 2820 の CLI が利用できるのは、スイッチで Enterprise Edition ソフトウェアが稼働している場合に限られます。

クラスタ コマンド スイッチの vty ラインにアクセス クラス コンフィギュレーションがある場合、このコマンドは機能しません。

クラスタ メンバ スイッチはクラスタ コマンド スイッチのパスワードを継承するため、クラスタ メンバ スイッチがクラスタに加入してもパスワードを要求するプロンプトは表示されません。

## 例

次の例では、メンバ 3 でセッションを開始する方法を示します。**exit** コマンドを入力するか、あるいはセッションを閉じるまで、このコマンドに続くすべてのコマンドは、メンバ 3 へ向けられます。

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

## 関連コマンド

| コマンド                                 | 説明                    |
|--------------------------------------|-----------------------|
| <a href="#">show cluster members</a> | クラスタ メンバに関する情報を表示します。 |

# remote-span

リモートスイッチドポートアナライザ (RSPAN) VLAN として VLAN を設定するには、VLAN コンフィギュレーションモードで **remote-span** 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。

## コマンドデフォルト

RSPAN VLAN は定義されません。

## コマンドモード

VLAN コンフィギュレーション (config-VLAN)

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

RSPAN VLAN を設定できるのは **config-vlan** モードの場合だけです (このモードは、**vlan** グローバルコンフィギュレーションコマンドで開始します)。**vlan database** 特権 EXEC コマンドを使用して開始された VLAN コンフィギュレーションモードでは設定できません。

VLAN トランキングプロトコル (VTP) がイネーブルで、VLAN ID が 1005 未満の場合は、RSPAN 機能は VTP によって伝達されます。RSPAN VLAN ID が拡張範囲内の場合は、手動で中間スイッチを設定する必要があります (送信元スイッチと宛先スイッチの間の RSPAN VLAN 内に設定)。

RSPAN **remote-span** コマンドを設定する前に、**vlan** (グローバルコンフィギュレーション) コマンドで VLAN を作成してください。

RSPAN VLAN には、次の特性があります。

- MAC アドレス ラーニングは実行されません。
- トランクポートでは RSPAN VLAN トラフィックだけが流れます。
- スパニングツリープロトコル (STP) は RSPAN VLAN 内では稼働できますが、RSPAN 宛先ポートでは稼働しません。

既存の VLAN が RSPAN VLAN として設定されている場合は、その VLAN が最初に削除され、RSPAN VLAN として再作成されます。アクセスポートは、RSPAN 機能がディセーブルになるまでは非アクティブです。

## 例

次の例では、RSPAN VLAN として VLAN を設定する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote-span
```

次の例では、VLAN から RSPAN 機能を削除する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# no remote-span
```

**show vlan remote-span** ユーザ EXEC コマンドを入力すると、設定を確認することができます。

## 関連コマンド

| コマンド                            | 説明  |
|---------------------------------|---|
| <a href="#">monitor session</a> | ポートでスイッチドポートアナライザ (SPAN) および RSPAN モニタリングをイネーブルにし、ポートを送信元ポートまたは宛先ポートとして設定します。 |
| <a href="#">vlan</a>            | 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、特権 EXEC モードで **renew ip dhcp snooping database** コマンドを使用します。

```
renew ip dhcp snooping database [{flash:/filename | ftp://user:password@host/filename |
nvrाम:/filename | rcp://user@host/filename | tftp://host/filename}] [validation none]
```

## 構文の説明

|  |   |
|--|---|
| <b>flash:/filename</b>                   | (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。                   |
| <b>ftp://user:password@host/filename</b> | (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。                    |
| <b>nvrाम:/filename</b>                   | (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。                     |
| <b>rcp://user@host/filename</b>          | (任意) データベース エージェントまたはバインディング ファイルがリモート コントロール プロトコル (RCP) サーバにあることを指定します。 |
| <b>tftp://host/filename</b>              | (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。                   |
| <b>validation none</b>                   | (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、巡回冗長検査 (CRC) を検証しないようにスイッチに指定します。 |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

URL を指定しない場合は、スイッチは設定された URL からファイルを読み込もうとします。

## 例

次の例では、ファイル内の CRC 値のチェックを省略して、DHCP スヌーピング バインディング データベースを更新する方法を示します。

```
Switch# renew ip dhcp snooping database validation none
```

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

## 関連コマンド

| コマンド   | 説明                                     |
|--|--|
| <a href="#">ip dhcp snooping</a>               | VLAN 上で DHCP スヌーピングをイネーブルにします。         |
| <a href="#">ip dhcp snooping binding</a>       | 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。      |
| <a href="#">show ip dhcp snooping database</a> | 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

REP の Resilient Ethernet Protocol (REP) 管理 VLAN を設定して、ハードウェア フラッドレイヤ (HFL) メッセージを送信するには、グローバル コンフィギュレーション モードで **rep admin vlan** 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。 |
|----------------|---|

## コマンドデフォルト

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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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ッディングします。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ッディングされます。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ッ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   |
|--|--|
| <a href="#">show interfaces rep detail</a> | 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) の VLAN ロード バランシングを設定するには、REP プライマリ エッジポートのインターフェイス コンフィギュレーション モードで **rep block port** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
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

|                        |  |
|------------------------|--|
| <b>id port-id</b>      | REP をイネーブルにすると自動的に生成される一意のポート ID を入力して VLAN ブロッキング代替ポートを指定します。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、 <b>show interface interface-id rep detail</b> コマンドを入力します。                        |
| <b>neighbor_offset</b> | 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。 |
| <b>preferred</b>       | VLAN ブロック代替ポートを、 <b>rep segment segment-id preferred</b> 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。<br><br>(注) <b>preferred</b> 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。                  |
| <b>vlan</b>            | ブロックされる VLAN を指定します。   |
| <b>vlan-list</b>       | 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。   |
| <b>all</b>             | すべての VLAN をブロックします。  |

## コマンド 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

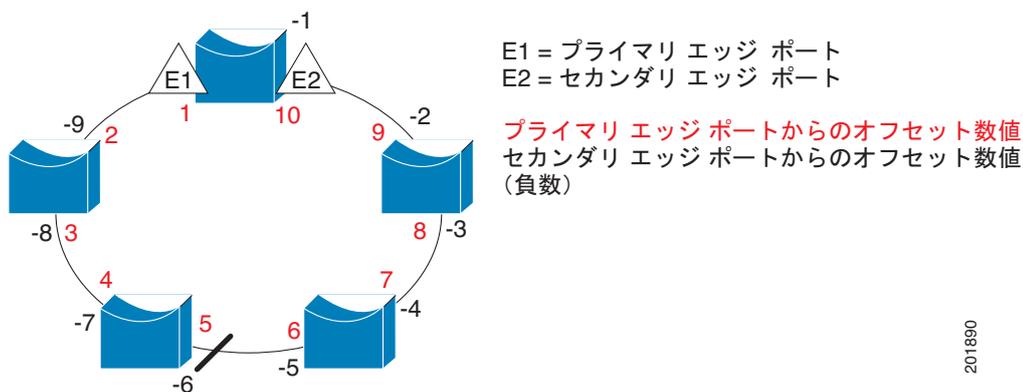
| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。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



(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ブ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ブ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ブ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 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 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 gigabitethernet1/2 rep detail
GigabitEthernet1/2 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
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 gigabitethernet1/1
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 gigabitethernet1/2
Switch (config-if)# rep block port 6 vlan 1-110
Switch (config-if)# end
```

```
Switch# show interface gigabitethernet1/2 rep detail
GigabitEthernet1/2 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   |
|-----------------------------------|--|
| <b>rep preempt delay</b>          | 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。         |
| <b>rep preempt segment</b>        | 手でセグメント上の REP VLAN ロード バランシングを開始します。                             |
| <b>show interfaces rep detail</b> | 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 タイマーを設定するには、Resilient Ethernet Protocol (REP) ポートのインターフェイス コンフィギュレーション モードで **rep lsl-age-timer** 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

*value* エージアウト時間 (ミリ秒)。指定できる範囲は 120 ms ~ 10000 ms で、40 ms ずつ増加します。デフォルト値は 5000 ミリ秒 (5 秒) です。

## コマンドデフォルト

REP リンクは、5000 ms 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せん。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

LSL エージ 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 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 15.0(1)EY 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 15.0(1)EY 以降が稼働していない場合、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。120 ミリ秒から 10000 ミリ秒に REP LSL エージング タイマーを設定できますが、ポート チャネルは、ポート チャネルの最小 LSL タイムアウト値である少なくとも 1000 ミリ秒 (1 秒) は継続します。

## 例

次の例では、REP リンクの REP LSL エージ タイマーを 7000 ms に設定する方法を示します。

```
Switch (config)# interface gigabitethernet1/2
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。

## 関連コマンド

| コマンド                                      | 説明   |
|---|--|
| <code>show interfaces rep [detail]</code> | 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 ポート障害とリカバリの後、Resilient Ethernet Protocol (REP) の 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 ポート上のインターフェイス コンフィギュレーション モードで **rep preempt delay** 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**

|              |   |
|--------------|---|
| <b>構文の説明</b> | <i>seconds</i> REP プリエンプションを遅延させる秒数。指定できる範囲は 15 ~ 300 です。 |
|--------------|---|

|                  |   |
|------------------|---|
| <b>コマンドデフォルト</b> | プリエンブション遅延は設定されていません。 <b>rep preempt delay</b> 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ブションとなります。 |
|------------------|---|

|                |                      |
|----------------|----------------------|
| <b>コマンドモード</b> | インターフェイス コンフィギュレーション |
|----------------|----------------------|

| <b>コマンド履歴</b> | リリース      | 変更内容            |
|---------------|-----------|-----------------|
|               | 15.0(1)EY | このコマンドが導入されました。 |

|                   |   |
|-------------------|---|
| <b>使用上のガイドライン</b> | 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。<br>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ブ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。

|          |   |
|----------|---|
| <b>例</b> | 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 gigabitethernet1/1
Switch (config-if)# rep preempt delay 100
Switch (config-if)# exit
```

| <b>関連コマンド</b> | コマンド                       | 説明  |
|---------------|----------------------------|---|
|               | <b>rep block port</b>      | VLAN ロード バランシングを設定します。                              |
|               | <b>show interfaces rep</b> | 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

手動で Resilient Ethernet Protocol (REP) の VLAN ロード バランシングをセグメントで開始するには、特権 EXEC モードで **rep preempt segment** 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 です。有効な範囲は 1 ~ 1024 です。

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 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   |
|-------------------------------------|--|
| <b>rep block port</b>               | VLAN ロード バランシングを設定します。                             |
| <b>show interfaces rep [detail]</b> | 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

インターフェイスの 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、インターフェイス コンフィギュレーション モードで **rep segment** 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>  | インターフェイスへのセグメント ID。有効な範囲は 1 ~ 1024 です。   |
| <b>edge</b>        | (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。<br><b>primary</b> キーワードなしで <b>edge</b> 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。  |
| <b>no-neighbor</b> | (任意) セグメント エッジを外部 REP ネイバーなしに設定します。  |
| <b>primary</b>     | (任意) エッジ ポートで、ポートがプライマリ エッジ ポートであることを指定します。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。 |
| <b>preferred</b>   | (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。<br><br>(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。                           |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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。

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
- トンネル ポート
- Access port

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。

近接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 トポロジ変更通知 (TCN) 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 gigabitethernet1/1
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 gigabitethernetv/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 gigabitethernet1/1
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 gigabitethernet1/2
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   |
|-------------------------------------|--|
| <b>show interfaces rep [detail]</b> | 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。           |
| <b>show rep topology [detail]</b>   | 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 セグメント トポロジ変更通知 (STCN) を他のインターフェイス、他のセグメントまたはスパンニングツリー プロトコル (STP) ネットワークに送信するポートを設定するには、Resilient Ethernet Protocol (REP) エッジポートのインターフェイス コンフィギュレーション モードで **rep stcn** 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

|                               |   |
|-------------------------------|---|
| <b>interface interface-id</b> | STCN を受信する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。  |
| <b>segment id-list</b>        | STCN を受信する REP セグメント 1 つまたは一連のセグメントを指定します。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。 |
| <b>stp</b>                    | STCN を STP ネットワークに送信します。  |

## コマンド 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 gigabitethernet1/2
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   |
|-------------------------------------|--|
| <b>show interfaces rep [detail]</b> | 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、DHCP プール コンフィギュレーション モードで **reserved-only** 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。

## コマンドデフォルト

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

DHCP プールの設定

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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)# ip dhcp pool test1
Switch(dhcp-config)# reserved-only
```

## 関連コマンド

| コマンド                     | 説明   |
|--------------------------|--|
| <b>show ip dhcp pool</b> | DHCP アドレス プールを表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

## rmon collection stats

ブロードキャストおよびマルチキャスト パケットについての活用統計情報と、巡回冗長検査 (CRC) アライメント エラーおよびコリジョンについてのエラー統計情報を含むイーサネット グループ統計情報を収集するには、インターフェイス コンフィギュレーション モードで **rmon collection stats** コマンドを使用します。デフォルト設定に戻すには、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 収集の所有者を指定します。  |

### コマンド デフォルト

RMON 統計情報収集はディセーブルです。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

RMON 統計情報収集コマンドはハードウェア カウンタに基づいています。

### 例

次の例では、所有者 `root` の RMON 統計情報を収集する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
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   |
|-----------------------------|--|
| <b>show rmon statistics</b> | RMON 統計情報を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# sdm prefer

Switch Database Management (SDM) リソース割り当てで使用されるテンプレートを設定するには、グローバル コンフィギュレーション モードで **sdm prefer** コマンドを使用します。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} | qos | routing}
```

```
no sdm prefer
```

## 構文の説明

|  |   |
|--|---|
| <b>default</b>                                   | すべてのレイヤ 2 機能を分散させます。  |
| <b>dual-ipv4-and-ipv6</b><br>{default   routing} | IPv4/IPv6 機能を分散させます。<br>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"> <li><b>default</b> : IPv4/IPv6 レイヤ 2 機能を分散させます。</li> <li><b>routing</b> : 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。レイヤ 3 機能を使用するには、IP サービス イメージが実行されているスイッチに IPv4 および IPv6 ルーティング テンプレートを使用します。</li> </ul> このテンプレートを設定して、IPv6 機能をイネーブルにする必要があります。 |
| <b>qos</b>                                       | 最大限のシステム使用率を Quality of Service (QoS) アクセス コントロール エントリ (ACE) に割り当てます。   |
| <b>routing</b>                                   | IPv4 ユニキャスト ルーティングのシステム使用率を最大限にします。レイヤ 3 機能の IP サービス イメージを実行しているスイッチではルーティング テンプレートを使用する必要があります。  |

## コマンド デフォルト

**default** テンプレートはすべての機能を均等に動作させます。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

スイッチをデフォルト テンプレートに設定するには、**no sdm prefer** コマンドを使用します。

レイヤ 3 機能を使用するには、IP サービス イメージが実行されているスイッチにルーティング テンプレートを使用します。

スイッチ上でレイヤ 3 機能ルーティングを使用しない場合は、ルーティング テンプレートを使用しないでください。**sdm prefer routing** グローバル コンフィギュレーション コマンドを入力することで、他の機能にルーティング テンプレートのユニキャスト ルーティングに割り当てたメモリを使用させないようにします。

スイッチで IPv6 機能をイネーブルにしない場合は、IPv4/IPv6 テンプレートを使用しないでください。**sdm prefer ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力すると、リソースを IPv4 と IPv6 に振り分けて、IPv4 フォワーディングに割り当てられたリソースを制限します。

表 2-16 では、IPv4 テンプレートそれぞれで利用できるリソースを示し、表 2-17 では、**dual-ipv4-and-ipv6** テンプレートの機能割り当てを示します。

表 2-16 各テンプレートに割り当てられた機能のリソースの概算

| リソース                  | デフォルト | QoS | ルーティン<br>グ |
|-----------------------|-------|-----|------------|
| ユニキャスト MAC アドレス       | 8 K   | 8 K | 2 K        |
| IGMP グループとマルチキャスト ルート | 256   | 256 | 1 K        |
| ユニキャスト ルート            | 0     |     | 4 K        |
| • ホストに直接接続            | 0     |     | 2 K        |
| • 間接ルート               | 0     |     | 2 K        |
| ポリシーベース ルーティング ACE    | 0     |     | 512        |
| QoS 分類 ACE            | 375   | 625 | 625        |
| セキュリティの ACE           | 375   | 125 | 375 K      |
| Layer 2 VLANs         | 1 K   | 1 K | 1 K        |

表の最初の 8 行（ユニキャスト MAC アドレスからセキュリティ ACE まで）は、各テンプレートが選択されたときに設定されるハードウェアのおおよその限度を表します。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。最後の行は、スイッチのレイヤ 2 VLAN の数に関連するハードウェア リソース消費量を計算するための目安です。

表 2-17 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<sup>1</sup>

| リソース                                  | IPv4 および<br>IPv6 のデフォ<br>ルト | IPv4 および<br>IPv6 のルー<br>ティン<br>グ |
|---------------------------------------|-----------------------------|----------------------------------|
| ユニキャスト MAC アドレス                       | 8 K                         | 1 K                              |
| IPv4 IGMP グループおよびマルチキャスト ルート          | 256                         | 512                              |
| IPv4 ユニキャスト ルートの合計：                   | 0                           | 2 K                              |
| • IPv4 ホストに直接接続                       | 0                           | 1 K                              |
| • 間接 IPv4 ルート                         | 0                           | 1 K                              |
| IPv6 マルチキャスト グループ                     | 375                         | 625                              |
| IPv6 ユニキャスト ルートの合計：                   | 0                           | 1375                             |
| • 直接接続された IPv6 アドレス                   | 0                           | 1 K                              |
| • 間接 IPv6 ユニキャスト ルート                  | 0                           | 375                              |
| IPv4 ポリシー ベース ルーティング ACE              | 0                           | 125                              |
| IPv4 または MAC QoS ACE (合計)             | 375                         | 375                              |
| IPv4 または MAC セキュリティの ACE (合計)         | 375                         | 125                              |
| IPv6 ポリシー ベース ルーティング ACE <sup>2</sup> | 0                           | 125                              |

表 2-17 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<sup>1</sup> (続き)

| 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 |
|------------------|----------------------|-----------------------|
| IPv6 QoS ACE     | 0                    | 125                   |
| IPv6 セキュリティの ACE | 125                  | 125                   |

1. この見積もりには、8 つのルーテッドインターフェイス、約 1000 個の VLAN が設定されたスイッチを使用しています。
2. IPv6 ポリシーベース ルーティングはサポートされません。

**例**

次の例では、QoS テンプレートの使用方法を示します。

```
Switch(config)# sdm prefer qos
Switch(config)# exit
Switch# reload
```

次の例では、スイッチ上でデフォルトのデュアル IPv4/IPv6 テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
```

次の例では、スイッチ上で IPv4/IPv6 ルーティング テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 routing
Switch(config)# exit
Switch# reload
Proceed with reload? [confirm]
```

**関連コマンド**

| コマンド                            | 説明  |
|---------------------------------|---|
| <a href="#">show sdm prefer</a> | 現在使用されている SDM テンプレート、または機能ごとのリソース割り当ての概算による使用可能なテンプレートを表示します。 |

# service password-recovery

パスワード回復メカニズム（デフォルト）をイネーブルにするには、グローバル コンフィギュレーション モードで **service password-recovery** コマンドを使用します。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。

**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。

## コマンド デフォルト

パスワード回復メカニズムはイネーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

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 **Express Setup** ボタンを押して起動プロセスを中断し、新しいパスワードを割り当てることができます。

パスワード回復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。

システム管理者は **no service password-recovery** コマンドを使用して、パスワード回復機能の一部をディセーブルにできます。これによりエンド ユーザは、システムをデフォルト設定に戻すことに同意した場合だけ、パスワードをリセットできます。

パスワード回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

スイッチのパスワードを削除して新しく設定するには、次の手順を実行します。

- ステップ 1** SETUP LED がグリーンに点滅し、使用可能なスイッチ ダウンリンク ポートの LED がグリーンに点滅するまで、[Express Setup] ボタンを押し続けます。

PC またはラップトップの接続に使用できるスイッチ ダウンリンク ポートの空きがない場合は、いずれかのスイッチ ダウンリンク ポートから装置を接続解除します。もう一度、SETUP LED とポートの LED がグリーンに点滅するまで [Express Setup] ボタンを押し続けます。
- ステップ 2** LED がグリーンに点滅しているポートに、PC またはラップトップを接続します。

SETUP LED とスイッチ ダウンリンク ポートの LED が点滅を中止し、グリーンに点灯します。
- ステップ 3** [Express Setup] ボタンを押し続けます。SETUP LED が再度グリーンに点滅し始めます。SETUP LED がグリーンに点灯するまで（約 5 秒間）、ボタンを押したままにします。すぐに [Express Setup] ボタンを放します。

この手順によって、他の設定に影響を与えることなく、パスワードが削除されます。これで、パスワードを入力せずに、コンソール ポートまたはデバイス マネージャからスイッチにアクセスできるようになりました。

**ステップ 4** デバイスマネージャの [Express Setup] ウィンドウを使用するか、コマンドラインインターフェイスで **enable secret** 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、新しいパスワードを入力します。

**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 **config** ファイルのコピーを保存しておくことを推奨します。スイッチ上に **config** ファイルのバックアップを保存しないでください。

スイッチが VTP トランスペアレントモードで動作している場合、**vlan.dat** ファイルもスイッチとは別の場所にコピーを保存しておくことを推奨します。

パスワードの回復がイネーブルかディセーブルかを確認するには、**show version** 特権 EXEC コマンドを入力します。

#### 例

次の例では、スイッチ上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                              |
|------------------------------|---------------------------------|
| <a href="#">show version</a> | ハードウェアおよびファームウェアのバージョン情報を表示します。 |

# service-policy

**policy-map** コマンドで定義されたポリシー マップを物理ポートまたはスイッチ仮想インターフェイス (SVI) の入力に適用するには、インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用します。ポリシー マップとポートの対応付けを削除するには、このコマンドの **no** 形式を使用します。

**service-policy input policy-map-name**

**no service-policy input policy-map-name**

## 構文の説明

**input policy-map-name** 物理ポートまたは SVI の入力に、指定したポリシー マップを適用します。



(注)

**history** キーワードは、コマンドラインのヘルプ スtringには表示されますが、サポートされていません。このキーワードが収集した統計情報は無視します。**output** キーワードもサポートされていません。

## コマンド デフォルト

ポートにポリシー マップは適用されていません。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

サポートされるポリシー マップは、入力ポートに 1 つだけです。

ポリシー マップは物理ポートまたは SVI で設定できます。物理ポートに **no mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用して VLAN ベース Quality of Service (QoS) をディセーブルにすると、ポートにポート ベースのポリシー マップを設定できます。**no mls qos vlan-based** インターフェイス コンフィギュレーション コマンドを使用して物理ポートで VLAN ベース QoS をイネーブルにすると、すでに設定済みのポート ベース ポリシー マップが削除されます。階層ポリシー マップを設定して SVI に適用すると、インターフェイス レベル ポリシー マップがインターフェイスに反映されます。

ポリシー マップは、物理ポートまたは SVI 上の着信トラフィックに適用できます。VLAN レベルのポリシー マップで定義された各クラスに対して、異なるインターフェイス レベル ポリシー マップを設定できます。階層ポリシー マップについては、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring QoS」の章を参照してください。

ポート信頼状態を使用した分類 (たとえば、**mls qos trust [cos | dscp | ip-precedence]**) とポリシー マップ (たとえば、**service-policy input policy-map-name**) は同時に指定できません。最後に行われた設定により、前の設定が上書きされます。

## 例

次の例では、物理入力ポートに plcmap1 を適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input plcmap1
```

次の例では、物理ポートから plcmap2 を削除する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no service-policy input plcmap2
```

次の例では、VLAN ベース QoS がイネーブルの場合に、入力 SVI に plcmap1 を適用する方法を示します。

```
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input plcmap1
```

次の例は、階層ポリシー マップを作成し、SVI に適用する方法を示しています。

```
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
.
.
.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input gigabitethernet1/1 - gigabitethernet1/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class-map cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)#exit
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class-map cm-1
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class-map cm-2
Switch(config-pmap-c)# match ip dscp 2
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap)# exit
Switch(config-pmap)# class-map cm-3
Switch(config-pmap-c)# match ip dscp 3
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap)# exit
Switch(config-pmap)# class-map cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)#
Switch(config-if)# ser input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
```

## 関連コマンド

| コマンド                       | 説明   |
|----------------------------|--|
| <b>policy-map</b>          | 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。  |
| <b>show policy-map</b>     | QoS ポリシー マップを表示します。  |
| <b>show running-config</b> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# set

パケットで DiffServ コードポイント (DSCP) または IP precedence 値を設定して IP トラフィックを分類するには、コンフィギュレーションモードで **set** ポリシーマップ クラス コマンドを使用します。トラフィックの分類を削除するには、このコマンドの **no** 形式を使用します。

```
set {dscp new-dscp | [ip] precedence new-precedence}
```

```
no set {dscp new-dscp | [ip] precedence new-precedence}
```

## 構文の説明

|                                       |  |
|---------------------------------------|--|
| <b>dscp new-dscp</b>                  | 分類されたトラフィックに割り当てられる新しい DSCP 値を指定します。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。            |
| <b>[ip] precedence new-precedence</b> | (任意) 分類されたトラフィックに割り当てる新しい IP precedence 値を指定します。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ック名を入力することもできます。 |

## コマンドデフォルト

トラフィックの分類は定義されていません。

## コマンドモード

ポリシー マップ クラス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**set ip dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用した場合は、スイッチによってこのコマンドはスイッチ コンフィギュレーションの **set dscp** に変更されます。**set ip dscp** ポリシー マップ クラス コンフィギュレーション コマンドを入力すると、スイッチ コンフィギュレーションではこの設定は **set dscp** として表示されます。

**set ip precedence** ポリシー マップ クラス コンフィギュレーション コマンドまたは **set precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。

同じポリシー マップ内では、**set** コマンドと **trust** ポリシー マップ クラス コンフィギュレーション コマンドを同時に指定できません。

**set dscp new-dscp** コマンドまたは **set ip precedence new-precedence** コマンドについては、一般的な値にニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力できます。これは **set dscp 10** コマンドの入力と同じです。**set ip precedence critical** コマンドを入力できます。これは **set ip precedence 5** コマンドの入力と同じです。サポートされるニーモニックのリストについては、**set dscp ?** または **set ip precedence ?** コマンドを入力して、コマンドラインのヘルプ スtring を表示してください。

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

## 例

次の例では、ポリサーが設定されていないすべての FTP トラフィックに DSCP 値 10 を割り当てる方法を示します。

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
```

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

## 関連コマンド

| コマンド                   | 説明   |
|------------------------|--|
| <b>class</b>           | 指定されたクラスマップ名のトラフィック分類一致条件 ( <b>police</b> 、 <b>set</b> 、および <b>trust</b> ポリシー マップ クラス コンフィギュレーション コマンドによる) を定義します。 |
| <b>police</b>          | 分類したトラフィックにポリサーを定義します。   |
| <b>policy-map</b>      | 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。   |
| <b>show policy-map</b> | QoS ポリシー マップを表示します。  |
| <b>trust</b>           | <b>class</b> ポリシー マップ コンフィギュレーション コマンドまたは <b>class-map</b> グローバル コンフィギュレーション コマンドを使用して分類されたトラフィックの信頼状態を定義します。      |

# setup

初期設定でスイッチを設定するには、特権 EXEC モードで **setup** 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。

### 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

**setup** コマンドを使用する場合、次の情報が必要になります。

- IP アドレスおよびネットワーク マスク
- 使用環境に対するパスワードの方針
- スイッチがクラスタ コマンド スイッチおよびクラスタ名として使用されるかどうか

**setup** コマンドを入力すると、System Configuration Dialog という対話形式のダイアログが表示されます。コンフィギュレーションプロセスが開始され、情報を求めるプロンプトが表示されます。各プロンプトの隣に表示されるカッコで囲まれた値は、**setup** コマンド機能または **configure** 特権 EXEC コマンドのいずれかを使用して設定された最後のデフォルト値です。

各プロンプトでヘルプ テキストが提供されます。ヘルプ テキストにアクセスするには、プロンプトで疑問符 (?) のキーを入力します。

変更を中断し、System Configuration Dialog を最後まで実行せずに特権 EXEC プロンプトに戻るには、Ctrl+C を押します。

変更が完了すると、セットアッププログラムにより、セットアップセッション中に作成されたコンフィギュレーション コマンド スクリプトが表示されます。設定を NVRAM に保存するか、あるいは設定を保存せずにセットアッププログラムまたはコマンドライン プロンプトに戻ることができます。

### 例

次の例では、**setup** コマンドの出力を示します。

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.
```

Would you like to enter basic management setup? [yes/no]: **yes**

Configuring global parameters:

Enter host name [Switch]: *host-name*

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret: *enable-secret-password*

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: *enable-password*

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: *terminal-password*

Configure SNMP Network Management? [no]: **yes**

Community string [public]:

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

| Interface | IP-Address     | OK? | Method | Status | Protocol |
|-----------|----------------|-----|--------|--------|----------|
| Vlan1     | 172.20.135.202 | YES | NVRAM  | up     | up       |

|                    |            |     |       |    |    |
|--------------------|------------|-----|-------|----|----|
| GigabitEthernet1/1 | unassigned | YES | unset | up | up |
|--------------------|------------|-----|-------|----|----|

|                    |            |     |       |    |      |
|--------------------|------------|-----|-------|----|------|
| GigabitEthernet1/2 | unassigned | YES | unset | up | down |
|--------------------|------------|-----|-------|----|------|

<output truncated>

|               |            |     |       |    |      |
|---------------|------------|-----|-------|----|------|
| Port-channel1 | unassigned | YES | unset | up | down |
|---------------|------------|-----|-------|----|------|

Enter interface name used to connect to the management network from the above interface summary: **vlan1**

Configuring interface vlan1:

Configure IP on this interface? [yes]: **yes**

IP address for this interface: *ip\_address*

Subnet mask for this interface [255.0.0.0]: *subnet\_mask*

Would you like to enable as a cluster command switch? [yes/no]: **yes**

Enter cluster name: *cluster-name*

The following configuration command script was created:

```
hostname host-name
enable secret 5 $1$LiBw$0XclwyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet1/1
no ip address
!
interface GigabitEthernet1/2
no ip address
```

## ■ setup

```

!

cluster enable cluster-name
!
end
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:

```

## 関連コマンド

| コマンド                       | 説明   |
|----------------------------|--|
| <b>show running-config</b> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show version</b>        | ハードウェアおよびファームウェアのバージョン情報を表示します。  |

# setup express

Express Setup モードをイネーブルにするには、グローバル コンフィギュレーション モードで **setup express** コマンドを使用します。Express Setup モードをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**setup express**

**no setup express**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンドデフォルト

Express Setup はイネーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

新しいスイッチ（未設定）上で Express Setup をイネーブルにする場合、Express Setup ボタンを 2 秒間押すことで Express Setup を開始できます。IP アドレス 10.0.0.1 を使用するとイーサネット ポート経由でスイッチにアクセスできます。その後、スイッチを Web ベースの Express Setup プログラム、またはコマンドライン インターフェイス（CLI）ベースのセットアップ プログラムで設定できます。

設定したスイッチで Express Setup ボタンを 2 秒間押すと、Express Setup ボタンの下にある LED が点滅し始めます。Express Setup ボタンを合計 10 秒間押すと、スイッチの設定は削除され、スイッチが再起動します。その場合、スイッチは、Web ベースの Express Setup プログラムまたは CLI ベースのセットアップ プログラムのいずれかで、新しいスイッチのように設定し直すことができます。



(注)

スイッチの設定に変更（CLI ベースのセットアップ プログラム開始時に **no** を入力することを含む）を行うとすぐに、Express Setup による設定を利用できなくなります。Express Setup ボタンを 10 秒間押し続けることによってのみ、再度 Express Setup を稼働できます。これにより、設定は削除され、スイッチが再起動します。

スイッチ上で Express Setup がアクティブな場合に、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを入力すると、Express Setup は非アクティブ化されます。スイッチの IP アドレス 10.0.0.1 は有効ではなくなり、この IP アドレスを使用している接続も終了します。

**no setup express** コマンドの主な目的は、Mode ボタンを 10 秒間押すことによってスイッチの設定が削除されるのを防ぐことです。

## 例

次の例では、Express Setup モードをイネーブルにする方法を示します。

```
Switch(config)# setup express
```

Express Setup ボタンを押すと、Express Setup モードがイネーブルであることを確認できます。

- 未設定のスイッチでは、Express Setup ボタンの下にある LED は 3 秒後にグリーンになります。
- 設定されたスイッチ上では、Mode の LED が 2 秒後に点滅し、10 秒後にグリーンになります。

**注意**

Express Setup ボタンを合計 10 秒間押し続けると、設定が削除され、スイッチが再起動します。

次の例では、Express Setup モードをディセーブルにする方法を示します。

```
Switch(config)# no setup express
```

Express Setup ボタンを押すと、Express Setup モードがディセーブルであることを確認できます。Express Setup モードがスイッチでイネーブルでない場合、LED はグリーンに点灯しないか、またはグリーンに点滅し始めます。

**関連コマンド**

| コマンド                               | 説明                                |
|------------------------------------|-----------------------------------|
| <a href="#">show setup express</a> | Express Setup モードがアクティブかどうか表示します。 |

# show access-lists

スイッチに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、特権 EXEC モードで **show access-lists** コマンドを使用します。

```
show access-lists [name | number | hardware counters | ipc]
```

| 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。                          |
| <b>hardware counters</b> | (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。         |
| <b>ipc</b>               | (任意) プロセス間通信 (IPC) プロトコル アクセス リスト コンフィギュレーションのダウンロード情報を表示します。 |

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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン** スイッチは IP 標準および拡張アクセス リストだけをサポートします。したがって、許可される数値は、1 ~ 199 と 1300 ~ 2699 だけです。

このコマンドでは、設定された MAC ACL も表示します。



(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。

例 次の例では、**show access-lists** コマンドの出力を示します。

```
Switch# show access-lists
Standard IP access list 1
 10 permit 1.1.1.1
 20 permit 2.2.2.2
 30 permit any
 40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
 10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
 10 permit 10.10.10.10
Extended IP access list 121
 10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
Extended IP access list CMP-NAT-ACL
Dynamic Cluster-HSRP deny ip any any
 10 deny ip any host 19.19.11.11
 20 deny ip any host 10.11.12.13
Dynamic Cluster-NAT permit ip any any
 10 permit ip host 10.99.100.128 any
 20 permit ip host 10.46.22.128 any
 30 permit ip host 10.45.101.64 any
 40 permit ip host 10.45.20.64 any
 50 permit ip host 10.213.43.128 any
 60 permit ip host 10.91.28.64 any
 70 permit ip host 10.99.75.128 any
 80 permit ip host 10.38.49.0 any
```

次の例では、**show access-lists hardware counters** コマンドの出力を示します。

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
Drop: All frame count: 855
Drop: All bytes count: 94143
Drop And Log: All frame count: 0
Drop And Log: All bytes count: 0
Bridge Only: All frame count: 0
Bridge Only: All bytes count: 0
Bridge Only And Log: All frame count: 0
Bridge Only And Log: All bytes count: 0
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0
Forwarded: All frame count: 2121
Forwarded: All bytes count: 180762
Forwarded And Log: All frame count: 0
Forwarded And Log: All bytes count: 0

L3 ACL INPUT Statistics
Drop: All frame count: 0
Drop: All bytes count: 0
Drop And Log: All frame count: 0
Drop And Log: All bytes count: 0
Bridge Only: All frame count: 0
Bridge Only: All bytes count: 0
Bridge Only And Log: All frame count: 0
Bridge Only And Log: All bytes count: 0
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0
Forwarded: All frame count: 13586
Forwarded: All bytes count: 1236182
Forwarded And Log: All frame count: 0
Forwarded And Log: All bytes count: 0
```

```

L2 ACL OUTPUT Statistics
  Drop: All frame count: 0
  Drop: All bytes count: 0
  Drop And Log: All frame count: 0
  Drop And Log: All bytes count: 0
  Bridge Only: All frame count: 0
  Bridge Only: All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU: All frame count: 0
  Forwarding To CPU: All bytes count: 0
  Forwarded: All frame count: 232983
  Forwarded: All bytes count: 16825661
  Forwarded And Log: All frame count: 0
  Forwarded And Log: All bytes count: 0

L3 ACL OUTPUT Statistics
  Drop: All frame count: 0
  Drop: All bytes count: 0
  Drop And Log: All frame count: 0
  Drop And Log: All bytes count: 0
  Bridge Only: All frame count: 0
  Bridge Only: All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU: All frame count: 0
  Forwarding To CPU: All bytes count: 0
  Forwarded: All frame count: 514434
  Forwarded: All bytes count: 39048748
  Forwarded And Log: All frame count: 0
  Forwarded And Log: All bytes count: 0

```

## 関連コマンド

| コマンド                            | 説明   |
|---------------------------------|--|
| <b>access-list</b>              | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>ip access-list</b>           | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>mac access-list extended</b> | 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、EXEC モードで **show alarm description port** コマンドを使用します。

## show alarm description port

### 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

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 例

次の例では、**show alarm description port** コマンドの出力例を示します。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   |
|---|--|
| <a href="#">alarm profile (グローバル コンフィギュレーション)</a> | 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。                           |
| <a href="#">show alarm profile</a>                | 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すべてのアラーム プロファイルまたは指定したプロファイルと、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表示するには、EXEC モードで、**show alarm profile** コマンドを使用します。

**show alarm profile** [*name*]

|          |             |                              |
|----------|-------------|------------------------------|
| 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。 |
| デフォルト    | なし          |                              |
| コマンド モード | EXEC        |                              |
| コマンド履歴   | リリース        | 変更内容                         |
|          | 15.0(1)EY   | このコマンドが導入されました。              |

**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。

**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      Gi1/2
Alarms         1,2,3,4
Syslog         1,2,3,4
Notifies       1,2,3,4
Relay-major    4
Relay-minor    1,2
```

## ■ show alarm profile

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      Gi1/2
Alarms         1,2,3,4
Syslog         1,2,3,4
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  |
|---|---|
| <b>alarm profile (グローバル<br/>コンフィギュレーション)</b>          | 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<br>プロファイルを作成します。 |
| <b>alarm profile (インターフェ<br/>イス コンフィギュレーショ<br/>ン)</b> | 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、EXEC モードで **show alarm settings** コマンドを使用します。

## show alarm settings

### 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

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 例

次の例では、**show alarm settings** コマンドの出力例を示します。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
Alarm relay mode: Positive
```

```
Power Supply
  Alarm           Enabled
  Relay           MAJ
  Notifies        Enabled
  Syslog          Enabled

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                  |
|---|---------------------|
| <a href="#">alarm facility power-supply</a> | 電源アラーム オプションを設定します。 |
| <a href="#">alarm facility temperature</a>  | 温度アラーム オプションを設定します。 |
| <a href="#">power-supply dual</a>           | デュアル電源モードを設定します。    |

# 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、特権 EXEC モードで **show archive status** コマンドを使用します。

## show archive status

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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は、**archive download-sw** コマンドの出力では、ダウンロードのステータスが表示されます。

TFTP サーバがない場合、HTTP を使用してイメージをダウンロードするには、Network Assistant または組み込みデバイス マネージャを使用します。**show archive status** コマンドでは、ダウンロードの進捗状況が表示されます。

### 例

次の例では、**show archive status** コマンドの出力を示します。

```
Switch# show archive status
IDLE: No upgrade in progress

Switch# show archive status
LOADING: Upgrade in progress

Switch# show archive status
EXTRACT: Extracting the image

Switch# show archive status
VERIFY: Verifying software

Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

### 関連コマンド

| コマンド                                | 説明                                |
|-------------------------------------|-----------------------------------|
| <a href="#">archive download-sw</a> | 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

アドレス解決プロトコル (ARP) のアクセス コントロール リストに関する詳細情報を表示するには、EXEC モードで **show arp access-list** コマンドを使用します。

```
show arp access-list [acl-name]
```

| 構文の説明     | <i>acl-name</i> (任意) ACL の名前です。   |      |      |           |                 |
|-----------|---|------|------|-----------|-----------------|
| デフォルト     | なし  |      |      |           |                 |
| コマンド モード  | EXEC  |      |      |           |                 |
| コマンド履歴    | <table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>15.0(1)EY</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 15.0(1)EY | このコマンドが導入されました。 |
| リリース      | 変更内容  |      |      |           |                 |
| 15.0(1)EY | このコマンドが導入されました。   |      |      |           |                 |

**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  |
|--------|--|---|
|        | <b>arp access-list</b>                   | ARP ACL を定義します。   |
|        | <b>deny (ARP アクセス リスト コンフィギュレーション)</b>   | 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。 |
|        | <b>ip arp inspection filter vlan</b>     | 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。                               |
|        | <b>permit (ARP アクセス リスト コンフィギュレーション)</b> | 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

スイッチの認証マネージャ イベントに関する情報を表示するには、**show authentication** コマンドを EXEC モードで使用します。

```
show authentication {interface interface-id | registrations | sessions [session-id session-id]
                    [handle handle] [interface interface-id] [mac mac] [method method] | statistics [summary]}
```

| 構文の説明                         |   |
|-------------------------------|---|
| <b>interface interface-id</b> | 指定したインターフェイスの認証マネージャの詳細をすべて表示します。   |
| <b>registrations</b>          | 認証マネージャの登録を表示します。   |
| <b>sessions</b>               | 現在の認証マネージャセッション（クライアントデバイスなど）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。 |
| <b>session-id session-id</b>  | （任意）認証マネージャのセッションを指定します。  |
| <b>handle handle</b>          | （任意）1 ~ 4294967295 の範囲を指定します。   |
| <b>mac mac</b>                | （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。  |
| <b>method method</b>          | （任意）指定した認証方式（ <b>dot1x</b> 、 <b>mab</b> 、または <b>webauth</b> ）によって許可されたクライアントをすべて表示します。  |
| <b>statistics</b>             | 認証統計情報の詳細を表示します。  |
| <b>summary</b>                | （任意）認証統計情報のサマリーを表示します。  |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

使用上のガイドライン 表 2-18 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テーブルに示します。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 2-18 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。        |
| 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。      |

表 2-18 show authentication コマンドの出力 (続き)

| フィールド         | 説明                           |
|---------------|------------------------------|
| 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 2-19 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 2-19 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       | Terminal | 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   | Terminal | 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 | Terminal | 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  | Terminal | 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

この例は、**show authentication registrations** コマンドの出力を示します

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
Handle Priority Name
3 0 dot1x
2 1 mab
1 2 webauth
```

この例は、**show authentication interface interface-id** コマンドの出力を示します。

```
Switch# show authentication interface gigabitethernet1/2
Client list:
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1//2
Available methods list:
Handle Priority Name
3 0 dot1x
Runnable methods list:
Handle Priority Name
3 0 dot1x
```

この例は、**show authentication sessions** コマンドの出力を示します。

```
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
```

この例は、指定されたインターフェイスの **show authentication sessions** コマンドの出力を示します。

```
Switch# show authentication sessions int gigabitethernet 1/4
```

## show authentication

```

Interface: GigabitEthernet0/46 GigabitEthernet1/4
MAC Address: Unknown
IP Address: Unknown
Status: Authz Success
Domain: DATA
Oper host mode: multi-host
Oper control dir: both
Authorized By: Guest Vlan
Vlan Policy: 4094
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 09081404000000080057c274
Acct Session ID: 0x0000000A
Handle: 0xCC000008
Runnable methods list:
Method State
dot1x Failed over

```

この例は、特定の MAC アドレスの **show authentication sessions** コマンドの出力を示します。

```

Switch# show authentication sessions mac 000e.84af.59bd
Interface: GigabitEthernet1/4
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

```

この例は、指定された方式の **show authentication session method** コマンド出力を示します。

```

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   |
|---|--|
| <b>authentication control-direction</b> | ポート モードを単一方向または双方向に設定します。  |
| <b>authentication event</b>             | 特定の認証イベントのアクションを設定します。   |
| <b>authentication fallback</b>          | 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。 |
| <b>authentication host-mode</b>         | ポートで認証マネージャ モードを設定します。   |
| <b>authentication open</b>              | 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。                                  |
| <b>authentication order</b>             | ポートで使用する認証方式の順序を設定します。   |
| <b>authentication periodic</b>          | 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。  |
| <b>authentication port-control</b>      | 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  |
|--------------------------------|---|
| <b>authentication priority</b> | ポートプライオリティ リストに認証方式を追加します。                |
| <b>authentication timer</b>    | 802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。 |

# show auto qos

自動 QoS (auto-QoS) がイネーブルのインターフェイスで入力された Quality of Service (QoS) コマンドを表示するには、**show auto qos** コマンドを EXEC モードで使用します。

```
show auto qos [interface [interface-id]]
```



(注) このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

**interface [interface-id]** (任意) 指定されたポートまたはすべてのポートの auto-QoS 情報を表示します。有効なインターフェイスには、物理ポートが含まれます。

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**show auto qos** コマンド出力には、各インターフェイスに入力された auto-QoS コマンドだけが表示されます。**show auto qos interface interface-id** コマンド出力は、特定のインターフェイスに入力された auto-QoS コマンドを表示します。

auto-QoS 設定およびユーザ変更を表示する場合は、**show running-config** 特権 EXEC コマンドを使用します。

**show auto qos** コマンド出力には、Cisco IP Phone のサービス ポリシー情報も表示されます。

auto-QoS の影響を受ける可能性のある現在の QoS の設定情報を表示するには、次のいずれかのコマンドを使用します。

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface [interface-id] [buffers | queueing]**
- **show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q | dscp-output-q]**
- **show mls qos input-queue**
- **show running-config**

## 例

次の例では、**auto qos voip cisco-phone** および **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos** コマンドの出力を示します。

```
Switch> show auto qos
```

```
GigabitEthernet1/1
auto qos voip cisco-softphone
```

```
GigabitEthernet1/3
auto qos voip cisco-phone
```

```
GigabitEthernet1/2
auto qos voip cisco-phone
```

次の例では、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos interface interface-id** コマンドの出力を示します。

```
Switch> show auto qos interface gigabitethernet 1/1
```

```
GigabitEthernet1/1
auto qos voip cisco-phone
```

次の例では、**auto qos voip cisco-phone** および **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show running-config** 特権 EXEC コマンドの出力を示します。

```
Switch# show running-config
Building configuration...
...
mls qos map policed-dscp 24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 75 75 75 250
mls qos queue-set output 1 threshold 3 75 150 100 300
```

## show auto qos

```

mls qos queue-set output 1 threshold 4 50 100 75 400
mls qos queue-set output 2 threshold 1 100 100 100 100
mls qos queue-set output 2 threshold 2 35 35 35 35
mls qos queue-set output 2 threshold 3 55 82 100 182
mls qos queue-set output 2 threshold 4 90 250 100 400
mls qos queue-set output 1 buffers 15 20 20 45
mls qos queue-set output 2 buffers 24 20 26 30
mls qos
...
!
class-map match-all AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp cs3  af31
!
policy-map AutoQoS-Police-SoftPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
!
policy-map AutoQoS-Police-CiscoPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
...
!
interface FastEthernet1/1
  switchport mode access
  switchport port-security maximum 1999
  speed 100
  duplex full
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  auto qos voip cisco-phone
!

interface GigabitEthernet1/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 2
  switchport mode access
  speed 10
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  auto qos voip cisco-phone
!

interface GigabitEthernet1/2
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  mls qos trust device cisco-phone
  service-policy input AutoQoS-Police-CiscoPhone

```

<output truncated>

次の例では、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos interface interface-id** コマンドの出力を示します。

```
Switch> show auto qos interface FastEthernet1/2
```

```
FastEthernet1/2  
auto qos voip cisco-softphone
```

次の例では、Auto-QoS がスイッチでディセーブルの場合の **show auto qos** コマンドの出力を示します。

```
Switch> show auto qos  
AutoQoS not enabled on any interface
```

次の例では、Auto-QoS がインターフェイスでディセーブルの場合の **show auto qos interface interface-id** コマンドの出力を示します。

```
Switch> show auto qos interface gigabitethernet1/1  
AutoQoS is disabled
```

#### 関連コマンド

| コマンド                           | 説明  |
|--------------------------------|---|
| <a href="#">auto qos voip</a>  | QoS ドメイン内の Voice over IP (VoIP) に QoS を自動設定します。 |
| <a href="#">debug auto qos</a> | auto-QoS 機能のデバッグをイネーブルにします。                     |

# show boot

BOOT 環境変数の設定を表示するには、特権 EXEC モードで **show boot** コマンドを使用します。

## show boot

### 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

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 例

次の例では、**show boot** コマンドの出力を示します。表 2-20 に、表示される各フィールドの説明を示します。

```
Switch# show boot
BOOT path-list      : flash:/ie2k-universalk9-mz.150-0.27.EY/ie2k-universalk9-mz
.150-0.27.EY.bin
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break       : yes
Manual Boot        : no
HELPER path-list   :
Auto upgrade       : yes
Auto upgrade path  :
Boot optimization  : enabled
NVRAM/Config file
  buffer size:     65536
Timeout for Config
  Download:        0 seconds
Config Download
  via DHCP:        disabled (next boot: disabled)
Switch#
```

表 2-20 show boot のフィールドの説明

| フィールド                         | 説明  |
|-------------------------------|---|
| BOOT path-list                | 自動起動時にロードおよび実行しようとする実行可能ファイルのセミコロン区切りリストを表示します。<br><br>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。<br><br>BOOT 環境変数が設定されていても指定されたイメージをロードできない場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとします。 |
| Config file                   | Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を表示します。   |
| Private Config file           | Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を表示します。   |
| Enable Break                  | 起動中のブレ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 Break キーを押すと、自動起動プロセスを中断できます。  |
| Manual Boot                   | スイッチが自動で起動するか、または手動で起動するかを表示します。no または 0 に設定されている場合、ブートローダはシステムを自動的に起動しようとします。それ以外に設定されている場合は、ブートローダ 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、ブートローダの機能を拡張したり、パッチを当てたりします。  |
| Auto upgrade                  | 非互換のスイッチに対して自動的にソフトウェア バージョンをコピーするようにスイッチが設定されているかを表示します。   |
| Boot optimization             | システム障害の発生後に、スイッチの起動時間を最適化するようにスイッチが設定されているかどうかを表示します。   |
| NVRAM/Config file buffer size | Cisco IOS がメモリ内のコンフィギュレーション ファイルのコピーを保持するために使用するバッファ サイズを表示します。コンフィギュレーションファイルは、バッファ サイズ割り当てを超えることはできません。   |

## 関連コマンド

| コマンド                            | 説明  |
|---------------------------------|---|
| <b>boot config-file</b>         | 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。   |
| <b>boot enable-break</b>        | 自動起動プロセスを中断できます。                                  |
| <b>boot manual</b>              | 次の起動サイクル時の手動スイッチ起動をイネーブルにします。                     |
| <b>boot private-config-file</b> | 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。 |
| <b>boot system</b>              | 次の起動サイクル中にロードする Cisco IOS イメージを指定します。             |

# show boot buffersize

ファイルシステムでシミュレートした NVRAM のバッファ サイズを表示するには、特権 EXEC モード **show boot buffersize** コマンドを使用します。

## show boot buffersize

### 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

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 例

次に、ファイルシステムでシミュレートした NVRAM のブート バッファ サイズを表示する例を示します。

```
Switch(config)# show boot buffersize
15000
Switch(config)#
```

### 関連コマンド

| コマンド                            | 説明                                       |
|---------------------------------|--|
| <a href="#">boot buffersize</a> | ファイルシステムでシミュレートした NVRAM のバッファ サイズを設定します。 |

# show cable-diagnostics tdr

タイムドメイン反射率計（TDR）の結果を表示するには、特権 EXEC モードで **show cable-diagnostics tdr** コマンドを使用します。

**show cable-diagnostics tdr interface *interface-id***

| 構文の説明      | <b>interface <i>interface-id</i></b> TDR が実行されているインターフェイス。  |      |      |           |                 |
|------------|---|------|------|-----------|-----------------|
| デフォルト      | なし  |      |      |           |                 |
| コマンドモード    | 特権 EXEC   |      |      |           |                 |
| コマンド履歴     | <table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>15.0(1)EY</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 15.0(1)EY | このコマンドが導入されました。 |
| リリース       | 変更内容  |      |      |           |                 |
| 15.0(1)EY  | このコマンドが導入されました。   |      |      |           |                 |
| 使用上のガイドライン | 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。  |      |      |           |                 |

例 次の例では、**show cable-diagnostics tdr interface *interface-id*** コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length Remote pair Pair status
-----
Gig1/2 auto Pair A 0 +/- 2 meters N/A Open
          Pair B 0 +/- 2 meters N/A Open
          Pair C 0 +/- 2 meters N/A Open
          Pair D 0 +/- 2 meters N/A Open
```

次の例では、**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 fa0/1
TDR test last run on: March 01 01:05:40
Interface Speed Local pair Pair length Remote pair Pair status
-----
Fa0/1 100M Pair A N/A Pair A Normal
          Pair B N/A Pair A Normal
          Pair C N/A Pair A N/A
          Pair D N/A Pair A N/A
```

## ■ show cable-diagnostics tdr

表 2-21 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 2-21 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って、TDR は場所を特定できます。 <ul style="list-style-type: none"> <li>ケーブルが正しく接続され、リンクがアップ状態で、インターフェイス速度が 1000 Mb/s である場合</li> <li>ケーブルが断線している場合</li> <li>ケーブルがショートしている場合</li> </ul>   |
| 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"> <li>Normal : ワイヤ ペアが正しく接続されています。</li> <li>Not completed : テストは実行中で、完了していません。</li> <li>Not supported : インターフェイスは TDR をサポートしません。</li> <li>Open : ワイヤ ペアが断線しています。</li> <li>Shorted : ワイヤ ペアがショートしています。</li> <li>ImpedanceMis : インピーダンスが一致しません。</li> <li>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。</li> <li>InProgress : 診断テストが進行中です。</li> </ul> |

次の例では、TDR が実行されているときの **show interfaces interface-id** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/2
gigabitethernet1/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が実行されていないときの **show cable-diagnostics tdr interface interface-id** コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/2
% TDR test was never issued on Gi1/2
```

インターフェイスで TDR がサポートされない場合、次のメッセージが表示されます。

```
% TDR test is not supported on switch 1
```

## 関連コマンド

| コマンド                              | 説明                            |
|-----------------------------------|-------------------------------|
| <b>test cable-diagnostics tdr</b> | インターフェイスで TDR をイネーブルにし、実行します。 |

# show cip

Common Industrial Protocol (CIP) サブシステムに関する情報を表示するには、特権 EXEC モードで **show cip** コマンドを使用します。

```
show cip {connection {count | explicit | implicit} | faults | file {config | eds | vlan} | miscellaneous
| object {assembly | dhcp instance instance | ethernet link | identity | switch {parameter} |
sync | tcp/ip {interface}} | security | session | status}
```

## 構文の説明

|                               |   |
|-------------------------------|---|
| <b>connection</b>             | CIP 接続情報を表示します。   |
| <b>count</b>                  | CIP 接続数を表示します。  |
| <b>explicit</b>               | 明示的な CIP 接続を表示します。  |
| <b>implicit</b>               | 暗黙的な CIP 接続を表示します。  |
| <b>faults</b>                 | CIP 障害に関する情報を表示します。   |
| <b>file</b>                   | CIP ファイル インスタンスに関する情報を表示します。  |
| <b>config</b>                 | コンフィギュレーション ファイルのインスタンスを表示します。  |
| <b>eds</b>                    | EDS ファイルのインスタンスを表示します。  |
| <b>vlan</b>                   | VLAN のファイルのインスタンスを表示します。  |
| <b>miscellaneous</b>          | 各種 CIP システム情報を表示します。  |
| <b>object</b>                 | 特定の CIP オブジェクトに関する情報を表示します。オブジェクトには、アセンブリ、イーサネット リンク、アイデンティティ、スイッチ パラメータ、時間同期および TCP/IP オブジェクトが含まれます。 |
| <b>assembly</b>               | CIP アセンブリのリンク オブジェクトを表示します。   |
| <b>dhcp instance instance</b> | 特定のインスタンスに関する DHCP オブジェクトを表示します。有効なインスタンスは、1 ~ 15 です。   |
| <b>ethernet link</b>          | CIP イーサネット オブジェクトを表示します。  |
| <b>identity</b>               | CIP アイデンティティ オブジェクトを表示します。  |
| <b>switch parameter</b>       | スイッチ パラメータを表示します。   |
| <b>sync</b>                   | CIP 時刻同期オブジェクトを表示します。   |
| <b>tcp/ip interface</b>       | TCP/IP オブジェクトを表示します。  |
| <b>security</b>               | CIP セキュリティ ウィンドウ ステータスおよび設定を表示します。  |
| <b>session</b>                | アクティブおよび非アクティブな CIP セッションを表示します。  |
| <b>status</b>                 | CIP ステータスを表示します (イネーブルまたはディセーブル)。   |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## show cip

## 例

次の例では、**show cip fault** コマンドの出力を示します。

```
Switch# show cip faults
Major/Minor Recoverable Faults
-----
MAC address flap : Normal
CDP native vlan mismatch : Normal
Storm control event : Normal
Port security violation : Normal
Port in error-disable state: Normal
Major Unrecoverable Faults
-----
POST detected HW failure : Normal
SFP in error-disable state : Normal
```

次の例では、**show cip security** コマンドの出力を示します。

```
Switch# show cip security
State : Enabled
Password: abc123
Window: Open
Owner IP: 172.20.140.147
Window timeout: 600 seconds
Window open tick: 17
```

## 関連コマンド

| コマンド                         | 説明                            |
|------------------------------|-------------------------------|
| <a href="#">cip enable</a>   | VLAN 上で CIP をイネーブルにします。       |
| <a href="#">cip security</a> | スイッチに CIP セキュリティ オプションを設定します。 |

# show cisp

指定されたインターフェイスの CISP 情報を表示するには、特権 EXEC モードで **show cisp** コマンドを使用します。

```
show cisp {[interface interface-id] | clients | summary}
```

| 構文の説明                                |   |
|--------------------------------------|---|
| <b>interface</b> <i>interface-id</i> | (任意) 指定されたインターフェイスの CISP 情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。 |
| <b>clients</b>                       | CISP クライアントの詳細を表示します。   |
| <b>summary</b>                       | すべての CISO 情報を表示します。   |

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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

例 次の例では、**show cisp interface** コマンドの出力を示します。

```
Switch# show cisp interface fast 0
CISP not enabled on specified interface
```

次の例では、**show cisp summary** コマンドの出力を示します。

```
Switch# show cisp summary
CISP is not running on any interface
```

| 関連コマンド | コマンド   | 説明  |
|--------|--|---|
|        | <b>cisp enable</b>   | Client Information Signalling Protocol (CISP) をイネーブルにします。 |
|        | <b>dot1x credentials (グローバル<br/>コンフィギュレーション)<br/>profile</b> | プロファイルをサブリカント スイッチに設定します。                                 |

# 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** コマンドを EXEC モードで使用します。

```
show class-map [class-map-name]
```

## 構文の説明

*class-map-name* (任意) 指定されたクラス マップの内容。

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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                                      |
|--|---|
| <a href="#">class-map</a>                  | 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。 |
| <a href="#">match (クラスマップ コンフィギュレーション)</a> | トラフィックを分類するための一致条件を定義します。               |

# show cluster

スイッチが属するクラスタのステータスおよびサマリーを表示するには、EXEC モードで **show cluster** コマンドを使用します。このコマンドは、クラスタ コマンド スイッチとクラスタ メンバ スイッチで入力できます。

## show cluster

### 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

なし

### コマンド モード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

クラスタのメンバでないスイッチ上でこのコマンドを入力すると、エラー メッセージ「Not a management cluster member」が表示されます。

クラスタ メンバ スイッチ上でこのコマンドを入力すると、クラスタ コマンド スイッチの ID、そのスイッチ メンバの番号、およびクラスタ コマンド スイッチとの接続状態が表示されます。

クラスタ コマンド スイッチ上でこのコマンドを入力すると、クラスタ名およびメンバの総数が表示されます。また、ステータス変更後のクラスタのステータスおよび時間も表示されます。冗長構成がイーネーブルの場合は、プライマリおよびセカンダリ コマンド スイッチの情報が表示されます。

### 例

次の例では、アクティブなクラスタ コマンド スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Command switch for cluster "cluster1
Total number of members:      7
Status:                       1 members are unreachable
Time since last status change: 0 days, 0 hours, 2 minutes
Redundancy:                   Enabled
    Standby command switch: Member 1
    Standby Group:            cluster1_standby
    Standby Group Number:    110
Heartbeat interval:          8
Heartbeat hold-time:        80
Extended discovery hop count: 3
```

次の例では、クラスタ メンバ スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch1> show cluster
Member switch for cluster "cluster2"
  Member number:          3
  Management IP address:  192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:    8
  Heartbeat hold-time:   80
```

次の例では、スタンバイ クラスタ コマンド スイッチとして設定されたクラスタ メンバ スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Member switch for cluster "hapuna"
  Member number:          3 (Standby command switch)
  Management IP address:  192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:    8
  Heartbeat hold-time:   80
```

次の例では、メンバ 1 との接続が切断されたクラスタ コマンド スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Command switch for cluster "Ajang"
  Total number of members: 7
  Status:                  1 members are unreachable
  Time since last status change: 0 days, 0 hours, 5 minutes
  Redundancy:              Disabled
  Heartbeat interval:      8
  Heartbeat hold-time:    80
  Extended discovery hop count: 3
```

次の例では、クラスタ コマンド スイッチとの接続が切断されたクラスタ メンバ スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Member switch for cluster "hapuna"
  Member number:          <UNKNOWN>
  Management IP address:  192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:    8
  Heartbeat hold-time:   80
```

## 関連コマンド

| コマンド                                    | 説明   |
|---|--|
| <a href="#">cluster enable</a>          | コマンド対応スイッチをクラスタ コマンド スイッチとしてイネーブルにし、クラスタ名、およびオプションとしてメンバ番号を割り当てます。 |
| <a href="#">show cluster candidates</a> | 候補スイッチのリストを表示します。  |
| <a href="#">show cluster members</a>    | クラスタ メンバに関する情報を表示します。  |

# show cluster candidates

候補スイッチのリストを表示するには、特権 EXEC モードで **show cluster candidates** コマンドを使用します。

**show cluster candidates [detail | mac-address H.H.H.]**

|       |                           |                              |
|-------|---------------------------|------------------------------|
| 構文の説明 | <b>detail</b>             | (任意) すべての候補に関する詳細情報を表示します。   |
|       | <b>mac-address H.H.H.</b> | (任意) クラスタ候補の MAC アドレスを指定します。 |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン** このコマンドは、クラスタ コマンド スイッチ上でだけ使用できます。スイッチがクラスタ コマンド スイッチでない場合は、プロンプトに空行が表示されます。出力内の SN は、**スイッチメンバ番号**を意味します。SN 列の値に E が表示された場合、スイッチは拡張検出によって検出されています。SN 列の値が E でない場合、**スイッチメンバ番号**のスイッチは、候補スイッチのアップストリーム側ネイバーです。ホップ カウントは、クラスタ コマンド スイッチから候補スイッチまでのデバイス数です。

**例** 次の例では、**show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates
00d0.7961.c4c0 StLouis-2 WS-IE2000-4TC Gi1/1 2 1 Fa1/1
00d0.bbf5.e900 ldf-dist-128 WS-C3524-XL Fa1/7 1 0 Fa0/24
00e0.1e7e.be80 1900_Switch 1900 3 0 1 0 Fa0/11
00e0.1e9f.7a00 Surfers-24 WS-C2924-XL Fa1/5 1 0 Fa0/3
00e0.1e9f.8c00 Surfers-12-2 WS-C2912-XL Fa1/4 1 0 Fa0/7
00e0.1e9f.8c40 Surfers-12-1 WS-C2912-XL Fa1/1 1 0 Fa0/9
```

次の例では、クラスタ コマンド スイッチに直接接続された、クラスタ メンバ スイッチの MAC アドレスを使用した場合の **show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates mac-address 00d0.7961.c4c0

Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
  Device type: cisco WS-IE2000-4TC
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 0)
  Local port: Gi1/1 FEC number:
  Upstream port: Gi2/2 FEC Number:
Hops from cluster edge: 1
Hops from command device: 1
```

## ■ show cluster candidates

次の例では、クラスタ エッジからのホップ カウントが 3 である、クラスタ メンバ スイッチの MAC アドレスを使用した場合の **show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
  Device type:          cisco WS-C2912MF-XL
  Upstream MAC address: 0010.7bb6.1cd4
  Local port:          Fa2/1   FEC number:
  Upstream port:      Fa0/24  FEC Number:
  Hops from cluster edge: 3
  Hops from command device: -
```

次の例では、**show cluster candidates detail** コマンドの出力を示します。

```
Switch> show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
  Device type:          cisco WS-C3512-XL
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 1)
  Local port:          Fa0/3   FEC number:
  Upstream port:      Fa0/13  FEC Number:
  Hops from cluster edge: 1
  Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
  Device type:          cisco 1900
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 2)
  Local port:          3       FEC number: 0
  Upstream port:      Fa0/11  FEC Number:
  Hops from cluster edge: 1
  Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
  Device type:          cisco WS-C2924-XL
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 3)
  Local port:          Fa0/5   FEC number:
  Upstream port:      Fa0/3   FEC Number:
  Hops from cluster edge: 1
  Hops from command device: 2
```

## 関連コマンド

| コマンド                                 | 説明                               |
|--------------------------------------|----------------------------------|
| <a href="#">show cluster</a>         | スイッチが属するクラスタのステータスおよびサマリーを表示します。 |
| <a href="#">show cluster members</a> | クラスタ メンバに関する情報を表示します。            |

# show cluster members

クラスタ メンバに関する情報を表示するには、特権 EXEC モードで **show cluster members** コマンドを使用します。

**show cluster members [n | detail]**

|       |   |
|-------|---|
| 構文の説明 | <i>n</i> (任意) クラスタ メンバを識別する番号。指定できる範囲は 0 ~ 15 です。 |
|       | <b>detail</b> (任意) すべてのクラスタ メンバに関する詳細を表示します。      |

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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

使用上のガイドライン このコマンドは、クラスタ コマンド スイッチ上でだけ使用できます。クラスタ内にメンバがない場合は、プロンプトに空行が表示されます。

例 次の例では、**show cluster members** コマンドの出力を示します。出力内の SN は、スイッチ番号を意味します。

```
Switch# show cluster members
          |---Upstream---|
SN MAC Address   Name           PortIf FEC Hops   SN PortIf FEC State
0  0002.4b29.2e00 StLouis1         0          0          Up (Cmdr)
1  0030.946c.d740 tal-switch-1    Fa0/13    1          0 Gi0/1    Up
2  0002.b922.7180 nms-2820       10        0          2          1 Fa0/18   Up
3  0002.4b29.4400 SanJuan2        Gi0/1     2          1 Fa0/11   Up
4  0002.4b28.c480 GenieTest       Gi0/2     2          1 Fa0/9    Up
```

次の例では、クラスタ メンバ 3 に対する **show cluster members** の出力を示します。

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
  Device type:          cisco WS-IE2000
  MAC address:          0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:          Gi1/1   FEC number:
  Upstream port:       Gi2/3   FEC Number:
  Hops from command device: 2
```

次の例では、**show cluster members detail** コマンドの出力を示します。

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
  Device type:          cisco WS-ies
  MAC address:          0002.4b29.2e00
  Upstream MAC address:
```

## show cluster members

```

Local port:                               FEC number:
Upstream port:                             FEC Number:
Hops from command device: 0
Device 'tal-switch-14' with member number 1
Device type:                               cisco WS-C3548-XL
MAC address:                               0030.946c.d740
Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
Local port:                               Fa0/13  FEC number:
Upstream port:                             Gi0/1   FEC Number:
Hops from command device: 1
Device 'nms-2820' with member number 2
Device type:                               cisco 2820
MAC address:                               0002.b922.7180
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:                               10     FEC number: 0
Upstream port:                             Fa0/18 FEC Number:
Hops from command device: 2
Device 'SanJuan2' with member number 3
Device type:                               cisco WS-ies
MAC address:                               0002.4b29.4400
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:                               Gi0/1  FEC number:
Upstream port:                             Fa0/11 FEC Number:
Hops from command device: 2
Device 'GenieTest' with member number 4
Device type:                               cisco SeaHorse
MAC address:                               0002.4b28.c480
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:                               Gi0/2  FEC number:
Upstream port:                             Fa0/9  FEC Number:
Hops from command device: 2
Device 'Palpatine' with member number 5
Device type:                               cisco WS-C2924M-XL
MAC address:                               00b0.6404.f8c0
Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
Local port:                               Gi2/1  FEC number:
Upstream port:                             Gi0/7  FEC Number:
Hops from command device: 1

```

## 関連コマンド

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

# show controllers cpu-interface

CPU ネットワーク インターフェイス ASIC のステートと、CPU に到達するパケットの送受信の統計情報を表示するには、特権 EXEC モードで **show controllers cpu-interface** コマンドを使用します。

## show controllers cpu-interface

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

なし

### コマンド モード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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。

### 例

次の例では、**show controllers cpu-interface** コマンドの出力を示します。

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped    invalid    hol-block
-----
rpc                4523063    0          0          0
stp                1545035    0          0          0
ipc                1903047    0          0          0
routing protocol  96145      0          0          0
L2 protocol        79596      0          0          0
remote console     0          0          0          0
sw forwarding      5756       0          0          0
host               225646     0          0          0
broadcast          46472      0          0          0
cbt-to-spt         0          0          0          0
igmp snooping     68411      0          0          0
icmp               0          0          0          0
logging            0          0          0          0
rpf-fail           0          0          0          0
queue14            0          0          0          0
cpu heartbeat      1710501    0          0          0
```

Supervisor ASIC receive-queue parameters

```
-----
queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
queue 3 maxrecevsize 5EE pakhead 19CDD00 paktail 19D02C8
```

<output truncated>

Supervisor ASIC Mic Registers

## ■ show controllers cpu-interface

```

-----
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   |
|--|--|
| <a href="#">show controllers ethernet-controller</a> | 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。 |
| <a href="#">show interfaces</a>                      | 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まれる各インターフェイスの送受信の統計情報を表示するには、キーワードを指定せずに特権 EXEC モードで **show controllers ethernet-controller** コマンドを使用します。

```
show controllers ethernet-controller [interface-id] [phy [detail]] [port-asic {configuration | statistics}] [fastethernet 0]
```

## 構文の説明

|                       |  |
|-----------------------|--|
| <b>interface-id</b>   | (任意) 物理インターフェイス (タイプ、モジュール、ポート番号を含む)。  |
| <b>phy</b>            | (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の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。 |
| <b>detail</b>         | (任意) PHY 内部レジスタの詳細情報を表示します。  |
| <b>port-asic</b>      | (任意) ポートの ASIC 内部レジスタの情報を表示します。  |
| <b>configuration</b>  | ポートの ASIC 内部レジスタの設定を表示します。   |
| <b>statistics</b>     | 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。  |
| <b>fastethernet 0</b> | (任意) ファストイーサネットの統計情報を表示します。  |

## デフォルト

なし

## コマンドモード

特権 EXEC (EXEC モードの *interface-id* 変数を指定した場合のみサポート)

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、すべてのインターフェイスまたは指定されたインターフェイスの基本的な RMON 統計情報を含むトラフィック統計情報をキーワードなしで表示します。

**phy** または **port-asic** キーワードを入力した場合は、主にシスコのテクニカルサポート担当によるスイッチのトラブルシューティングに役立つ情報が表示されます。

## 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 2-22 に Transmit フィールドの説明を示し、表 2-23 に Receive フィールドの説明を示します。

```
Switch# show controllers ethernet-controller gigabitethernet1/1
Transmit GigabitEthernet1/1          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 2-22 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 2-22 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 <sup>1</sup> 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 2-23 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 <sup>1</sup> 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 2-23 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 <sup>2</sup> 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 (最大伝送単位)

次の例では、特定のインターフェイスに対する **show controllers ethernet-controller phy** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller gigabitethernet1/1 phy
GigabitEthernet1/1 (gpn: 1, port-number: 1)
```

```
-----
General SFP Information
```

```
-----
Identifier          : 0x03
Connector           : 0x00
Transceiver         : 0x00 0x00 0x00 0x08 0x00 0x00 0x00 0x00
Encoding            : 0x01
BR_Nominal          : 0x0D
Vendor Name         : CISCO-METHODE
Vendor Part Number  : SP7041
Vendor Revision     : 0x43 0x20 0x20 0x20
Vendor Serial Number : 00000MTC1017075F
-----
```

```
-----
Other Information
```

```
-----
Port asic num       : 0
Port asic port num  : 0
XCVR init completed : 0
Embedded PHY        : not present
```

```
SFP presence index : 0
SFP iter cnt        : 30
SFP failed oper flag : 0x0
IIC error cnt       : 0
IIC error dsb cnt   : 0
IIC max sts cnt     : 50
Chk for link status : 1
Link Status         : 1
Link Status Media   : 2
```

次の例では、**show controllers ethernet-controller port-asic configuration** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller port-asic configuration
```

```
=====
Switch 1, PortASIC 0 Registers
```

```
-----
DeviceType          : 000101BC
Reset               : 00000000
PmadMicConfig       : 00000001
PmadMicDiag         : 00000003
SupervisorReceiveFifoSramInfo : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo : 000001D0 000001D0 40000000
GlobalStatus        : 00000800
IndicationStatus    : 00000000
IndicationStatusMask : FFFFFFFF
InterruptStatus     : 00000000
InterruptStatusMask : 01FFE800
SupervisorDiag      : 00000000
SupervisorFrameSizeLimit : 000007C8
SupervisorBroadcast : 000A0F01
GeneralIO           : 000003F9 00000000 00000004
StackPcsInfo        : FFFF1000 860329BD 5555FFFF FFFFFFFF
                    : FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo        : 73001630 00000003 7F001644 00000003
                    : 24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus  : 18E418E0
```

## show controllers ethernet-controller

```

stackControlStatusMask          : FFFFFFFF
TransmitBufferFreeListInfo      : 00000854 00000800 00000FF8 00000000
                                0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo           : 00000016 00000016 40000000 00000000
                                0000000C 0000000C 40000000 00000000
TransmitBufferInfo             : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount      : 00000F7A
TransmitBufferCommonCountPeak  : 0000001E
TransmitBufferCommonCommonEmpty : 000000FF
NetworkActivity                 : 00000000 00000000 00000000 02400000
DroppedStatistics              : 00000000
FrameLengthDeltaSelect         : 00000001
SneakPortFifoInfo             : 00000000
MacInfo                         : 0EC0801C 00000001 0EC0801B 00000001
                                00C0001D 00000001 00C0001E 00000001

```

<output truncated>

次の例では、**show controllers ethernet-controller port-asic statistics** コマンドの出力を示します。

```

Switch# show controllers ethernet-controller port-asic statistics
=====
Switch 1, PortASIC 0 Statistics
-----
      0 RxQ-0, wt-0 enqueue frames          0 RxQ-0, wt-0 drop frames
4118966 RxQ-0, wt-1 enqueue frames         0 RxQ-0, wt-1 drop frames
      0 RxQ-0, wt-2 enqueue frames         0 RxQ-0, wt-2 drop frames

      0 RxQ-1, wt-0 enqueue frames          0 RxQ-1, wt-0 drop frames
    296 RxQ-1, wt-1 enqueue frames         0 RxQ-1, wt-1 drop frames
2836036 RxQ-1, wt-2 enqueue frames         0 RxQ-1, wt-2 drop frames

      0 RxQ-2, wt-0 enqueue frames          0 RxQ-2, wt-0 drop frames
      0 RxQ-2, wt-1 enqueue frames         0 RxQ-2, wt-1 drop frames
158377 RxQ-2, wt-2 enqueue frames         0 RxQ-2, wt-2 drop frames

      0 RxQ-3, wt-0 enqueue frames          0 RxQ-3, wt-0 drop frames
      0 RxQ-3, wt-1 enqueue frames         0 RxQ-3, wt-1 drop frames
      0 RxQ-3, wt-2 enqueue frames         0 RxQ-3, wt-2 drop frames

15 TxBufferFull Drop Count                0 Rx Fcs Error Frames
      0 TxBufferFrameDesc BadCrc16         0 Rx Invalid Oversize Frames
      0 TxBuffer Bandwidth Drop Cou        0 Rx Invalid Too Large Frames
      0 TxQueue Bandwidth Drop Coun        0 Rx Invalid Too Large Frames
      0 TxQueue Missed Drop Statist        0 Rx Invalid Too Small Frames
74 RxBuffer Drop DestIndex Cou            0 Rx Too Old Frames
      0 SneakQueue Drop Count              0 Tx Too Old Frames
      0 Learning Queue Overflow Fra        0 System Fcs Error Frames
      0 Learning Cam Skip Count

15 Sup Queue 0 Drop Frames                 0 Sup Queue 8 Drop Frames
      0 Sup Queue 1 Drop Frames            0 Sup Queue 9 Drop Frames
      0 Sup Queue 2 Drop Frames            0 Sup Queue 10 Drop Frames
      0 Sup Queue 3 Drop Frames            0 Sup Queue 11 Drop Frames
      0 Sup Queue 4 Drop Frames            0 Sup Queue 12 Drop Frames
      0 Sup Queue 5 Drop Frames            0 Sup Queue 13 Drop Frames
      0 Sup Queue 6 Drop Frames            0 Sup Queue 14 Drop Frames
      0 Sup Queue 7 Drop Frames            0 Sup Queue 15 Drop Frames
=====
Switch 1, PortASIC 1 Statistics
-----
      0 RxQ-0, wt-0 enqueue frames          0 RxQ-0, wt-0 drop frames
      52 RxQ-0, wt-1 enqueue frames        0 RxQ-0, wt-1 drop frames

```

```
0 RxQ-0, wt-2 enqueue frames          0 RxQ-0, wt-2 drop frames  
<output truncated>
```

**関連コマンド**

| コマンド   | 説明  |
|--|---|
| <a href="#">show controllers<br/>cpu-interface</a> | 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。   |
| <a href="#">show controllers power<br/>inline</a>  | 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** コマンドを EXEC モードで使用します。

**show controllers power inline** [*instance*]

## 構文の説明

*instance* (任意) 電源コントローラのインスタンス。各インスタンスは 4 つのポートに対応します。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。

## コマンドモード

ユーザ EXEC  
特権 EXEC

## コマンド履歴

| リリース       | 変更内容            |
|------------|-----------------|
| 15.0(2)EY1 | このコマンドが追加されました。 |

## 使用上のガイドライン

インスタンスの範囲は 0 ~ 1 です。0 ~ 1 以外のインスタンスでは、スイッチは出力を提供しません。インスタンスがすべてのスイッチに表示されますが、このコマンドは、PoE スイッチだけで有効です。コマンドは PoE をサポートしないスイッチの情報は提供しません。

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。

## 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
Controller Instance 0, Address 0x50
```

```
Standard Registers:
```

```
-----
Interrupt           Reg 0x0  = 0x8
Intr Mask           Reg 0x1  = 0xF6
Power Event         Reg 0x2  = 0x0
Detect Event        Reg 0x4  = 0x1
Fault Event         Reg 0x6  = 0x0
T-Start Event       Reg 0x8  = 0x0
Supply Event        Reg 0xA  = 0x0
Port 1 Status       Reg 0xC  = 0x6
Port 3 Status       Reg 0xD  = 0x6
Port 5 Status       Reg 0xE  = 0x6
Port 7 Status       Reg 0xF  = 0x6
Power Status        Reg 0x10 = 0x0
Pin Status          Reg 0x11 = 0x20
Operating Mode      Reg 0x12 = 0xAA
Disconnect Enable   Reg 0x13 = 0xF
Detect/Class Enable Reg 0x14 = 0xFF
Reserved           Reg 0x15 = 0x0
Timing Config       Reg 0x16 = 0x0
Misc Config         Reg 0x17 = 0x80
```

```

ID Revision          Reg 0x1B = 0x41

Extended Registers:
-----
Port 1 :
  Police Value       Reg 0x1E = 0xF
  IEEE Type1 Penable Reg 0x23 = no
  IEEE Type2 Penable Reg 0x23 = no
  IEEE Power On Fault Reg 0x24 = No Fault
  2XPow Enabled      Reg 0x40 = no
  ICUT               Reg 0x2A = 352 mA
  Current            Reg 0x30/31 = 0
  Voltage            Reg 0x32/33 = 0

Port 3:
  Police Value       Reg 0x1E = 0xF
  IEEE Type1 Penable Reg 0x23 = no
  IEEE Type2 Penable Reg 0x23 = no
  IEEE Power On Fault Reg 0x24 = No Fault
  2XPow Enabled      Reg 0x40 = no
  ICUT               Reg 0x2A = 352 mA
  Current            Reg 0x34/35 = 0
  Voltage            Reg 0x36/37 = 0

Port 5:
  Police Value       Reg 0x1F = 0xF
  IEEE Type1 Penable Reg 0x23 = no
  IEEE Type2 Penable Reg 0x23 = no
  IEEE Power On Fault Reg 0x24 = No Fault
  2XPow Enabled      Reg 0x40 = no
  ICUT               Reg 0x2B = 352 mA
  Current            Reg 0x38/39 = 0
  Voltage            Reg 0x3A/3B = 0

Port 7:
  Police Value       Reg 0x1F = 0xF
  IEEE Type1 Penable Reg 0x23 = no
  IEEE Type2 Penable Reg 0x23 = no
  IEEE Power On Fault Reg 0x24 = No Fault
  2XPow Enabled      Reg 0x40 = no
  ICUT               Reg 0x2B = 352 mA
  Current            Reg 0x3C/3D = 0
  Voltage            Reg 0x3E/3F = 0

MCU temperature     Reg 0x2C = 86
Vee Voltage         Reg 0x2E/2F = 9285
Firmware Revision   Reg 0x41 = 32
WdogTimer Disable   Reg 0x42 = 11
WdogTimer Status    Reg 0x42 = 0
DeviceID            Reg 0x43 = 5
SiliconRevision     Reg 0x43 = 5

```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">logging event power-inline-status</a> | PoE イベントのロギングをイネーブルにします。                      |
| <a href="#">power inline</a>                      | 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。    |
| <a href="#">show profinet</a>                     | 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) と、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、特権 EXEC モードで **show controllers tcam** コマンドを使用します。

**show controllers tcam [asic [number]] [detail]**

## 構文の説明

|               |  |
|---------------|--|
| <b>asic</b>   | (任意) ポート ASIC TCAM 情報を表示します。                       |
| <b>number</b> | (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。 |
| <b>detail</b> | (任意) TCAM レジスタの詳細情報を表示します。                         |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 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   |
|--|--|
| <a href="#">show controllers cpu-interface</a>       | 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。        |
| <a href="#">show controllers ethernet-controller</a> | 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、EXEC モードで **show controllers utilization** コマンドを使用します。

**show controllers** [*interface-id*] **utilization**

## 構文の説明

*interface-id* (任意) スイッチ インターフェイスの ID です。

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例は、**show controllers utilization** コマンドの出力を示しています。

```
Switch> show controllers utilization
Port          Receive Utilization  Transmit Utilization
Fa1/1         0                    0
Fa1/2         0                    0
Fa1/3         0                    0
Fa1/4         0                    0
Fa1/5         0                    0
Fa1/6         0                    0
Fa1/7         0                    0
<output truncated>

<output truncated>

Switch Receive Bandwidth Percentage Utilization : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Switch Fabric Percentage Utilization : 0
```

次の例では、特定のポートでの **show controllers utilization** コマンドの出力を示します。

```
Switch> show controllers gigabitethernet1/1 utilization
Receive Bandwidth Percentage Utilization : 0
Transmit Bandwidth Percentage Utilization : 0
```

表 2-24 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                     |
|---|------------------------|
| <code>show controllers ethernet-controller</code> | インターフェイスの内部レジスタを表示します。 |

# 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、動作ステータスを表示するには、EXEC モードで **show dot1x** をコマンド使用します。

```
show dot1x [{all [summary] | interface interface-id} [details | statistics]]
```

## 構文の説明

|                               |   |
|-------------------------------|---|
| <b>all summary</b>            | (任意) すべてのポートの IEEE 802.1x ステータスを表示します。                      |
| <b>interface interface-id</b> | (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 ステータスを表示します。 |
| <b>details</b>                | (任意) IEEE 802.1x インターフェイスの詳細を表示します。                         |
| <b>statistics</b>             | (任意) 指定されたポートの IEEE 802.1x 統計情報を表示します。                      |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

ポートを指定しない場合は、グローバル パラメータおよびサマリーが表示されます。ポートを指定する場合、ポートの詳細が表示されます。

単一方向または双方向の制御としてポート制御が設定され、この設定がスイッチの設定と対立する場合は、**show dot1x {all | interface interface-id}** 特権 EXEC コマンド出力にその情報が表示されます。

```
ControlDirection = In (Inactive)
```

## 例

次の例では、**show dot1x EXEC** コマンドの出力を示します。

```
Switch> show dot1x
Sysauthcontrol          Enabled
Dot1x Protocol Version      2
Critical Recovery Delay    100
Critical EAPOL           Disabled
```

次の例では、**show dot1x all EXEC** コマンドの出力を示します。

```
Switch> show dot1x all
Sysauthcontrol          Enabled
Dot1x Protocol Version      2
Critical Recovery Delay    100
Critical EAPOL           Disabled

Dot1x Info for GigabitEthernet1/1
-----
PAE                      = AUTHENTICATOR
PortControl              = AUTO
ControlDirection        = Both
```

```

HostMode                = SINGLE_HOST
Violation Mode          = PROTECT
ReAuthentication        = Disabled
QuietPeriod             = 60
ServerTimeout           = 30
SuppTimeout            = 30
ReAuthPeriod           = 3600 (Locally configured)
ReAuthMax               = 2
MaxReq                  = 2
TxPeriod                = 30
RateLimitPeriod        = 0

```

<output truncated>

次の例では、**show dot1x all summary EXEC** コマンドの出力を示します。

| Interface | PAE  | Client         | Status       |
|-----------|------|----------------|--------------|
| Gi1/1     | AUTH | none           | UNAUTHORIZED |
| Gi1/2     | AUTH | 00a0.c9b8.0072 | AUTHORIZED   |
| Fa1/1     | AUTH | none           | UNAUTHORIZED |

次の例では、**show dot1x interface interface-id EXEC** コマンドの出力を示します。

```

Switch> show dot1x interface gigabitethernet1/2
Dot1x Info for GigabitEthernet1/2
-----
PAE                = AUTHENTICATOR
PortControl        = AUTO
ControlDirection  = In
HostMode           = SINGLE_HOST
ReAuthentication   = Disabled
QuietPeriod       = 60
ServerTimeout     = 30
SuppTimeout       = 30
ReAuthPeriod      = 3600 (Locally configured)
ReAuthMax         = 2
MaxReq            = 2
TxPeriod          = 30
RateLimitPeriod   = 0

```

次の例では、**show dot1x interface interface-id details EXEC** コマンドの出力を示します。

```

Switch# show dot1x interface gigabitethernet1/2 details
Dot1x Info for GigabitEthernet1/2
-----
PAE                = AUTHENTICATOR
PortControl        = AUTO
ControlDirection  = Both
HostMode           = SINGLE_HOST
ReAuthentication   = Disabled
QuietPeriod       = 60
ServerTimeout     = 30
SuppTimeout       = 30
ReAuthPeriod      = 3600 (Locally configured)
ReAuthMax         = 2
MaxReq            = 2
TxPeriod          = 30
RateLimitPeriod   = 0

Dot1x Authenticator Client List Empty

```

次の例では、ポートがゲスト VLAN に割り当てられ、ホスト モードが `multiple-hosts` モードに変更された場合の `show dot1x interface interface-id details` コマンドの出力を示します。

```
Switch# show dot1x interface gigabitEthernet1/1 details
Dot1x Info for GigabitEthernet1/1
-----
PAE                               = AUTHENTICATOR
PortControl                       = AUTO
ControlDirection                 = Both
HostMode                          = SINGLE_HOST
ReAuthentication                  = Enabled
QuietPeriod                      = 60
ServerTimeout                    = 30
SuppTimeout                      = 30
ReAuthPeriod                     = 3600 (Locally configured)
ReAuthMax                         = 2
MaxReq                           = 2
TxPeriod                         = 30
RateLimitPeriod                  = 0
Guest-Vlan                       = 182

Dot1x Authenticator Client List Empty

Port Status                       = AUTHORIZED
Authorized By                     = Guest-Vlan
Operational HostMode             = MULTI_HOST
Vlan Policy                      = 182
```

次の例では、`show dot1x interface interface-id statistics` 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。

```
Switch> show dot1x interface gigabitEthernet1/2 statistics
Dot1x Authenticator Port Statistics for GigabitEthernet1/2
-----
RxStart = 0      RxLogoff = 0      RxResp = 1      RxRespID = 1
RxInvalid = 0   RxLenErr = 0      RxTotal = 2

TxReq = 2      TxReqID = 132   TxTotal = 134

RxVersion = 2   LastRxSrcMAC = 00a0.c9b8.0072
```

表 2-25 show dot1x statistics のフィールドの説明

| フィールド      | 説明   |
|------------|--|
| RxStart    | 受信された有効な Extensible Authentication Protocol over LAN (EAPOL) -Start フレームの数                     |
| RxLogoff   | 受信された EAPOL-Logoff フレームの数  |
| RxResp     | 受信された有効な Extensible Authentication Protocol (EAP) -Response フレーム (Response/Identity フレーム以外) の数 |
| RxRespID   | 受信された EAP-Response/Identity フレームの数   |
| RxInvalid  | 受信された EAPOL フレームのうち、フレーム タイプを認識できないフレームの数  |
| RxLenError | 受信された EAPOL フレームのうち、パケット本体の長さを示すフィールドが無効なフレームの数  |
| RxTotal    | 受信されたすべてのタイプの有効な EAPOL フレームの数  |
| TxReq      | 送信された EAP-Request フレーム (Request/Identity フレーム以外) の数  |

表 2-25 show dot1x statistics のフィールドの説明 (続き)

| 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  |
| TxTotal      | 送信されたすべてのタイプの Extensible Authentication Protocol over LAN (EAPOL) フレームの数 |
| RxVersion    | IEEE 802.1x バージョン 1 形式で受信されたパケットの数                                       |
| LastRxSrcMac | 最後に受信した EAPOL フレームで伝送された送信元 MAC アドレス                                     |

## 関連コマンド

| コマンド                          | 説明                             |
|-------------------------------|--------------------------------|
| <a href="#">dot1x default</a> | IEEE 802.1x パラメータをデフォルト値に戻します。 |

# show dtp

スイッチまたは指定されたインターフェイスのダイナミック トランッキング プロトコル (DTP) の情報を表示するには、特権 EXEC モードで **show dtp** コマンドを使用します。

**show dtp** [*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) を含みません。

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、**show dtp** コマンドの出力を示します。

```
Switch# show dtp
Global DTP information
  Sending DTP Hello packets every 30 seconds
  Dynamic Trunk timeout is 300 seconds
  21 interfaces using DTP
```

次の例では、**show dtp interface** コマンドの出力を示します。

```
Switch# show dtp interface gigabitethernet1/1
DTP information for GigabitEthernet1/1:
  TOS/TAS/TNS:                ACCESS/AUTO/ACCESS
  TOT/TAT/TNT:                NATIVE/NEGOTIATE/NATIVE
  Neighbor address 1:          000943A7D081
  Neighbor address 2:          000000000000
  Hello timer expiration (sec/state): 1/RUNNING
  Access timer expiration (sec/state): never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state): never/STOPPED
  FSM state:                   S2:ACCESS
  # times multi & trunk        0
  Enabled:                      yes
  In STP:                       no

Statistics
-----
3160 packets received (3160 good)
0 packets dropped
  0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
6320 packets output (6320 good)
  3160 native
0 output errors
0 trunk timeouts
1 link ups, last link up on Mon Mar 01 1993, 01:02:29
```

```
0 link downs
```

---

**関連コマンド**

| コマンド                                  | 説明                      |
|---------------------------------------|-------------------------|
| <a href="#">show interfaces trunk</a> | インターフェイス トランク 情報を表示します。 |

# show eap

スイッチまたは指定されたポートの拡張認証プロトコル (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するには、特権 EXEC モードで **show eap** コマンドを使用します。

```
show eap {{registrations [method [name] | transport [name]]} | {sessions [credentials name
[interface interface-id] | interface interface-id | method name | transport name]} }
[credentials name | interface interface-id | transport name]
```

## 構文の説明

|                               |  |
|-------------------------------|--|
| <b>registrations</b>          | EAP レジストレーション情報を表示します。                           |
| <b>method name</b>            | (任意) EAP 方式のレジストレーション情報を表示します。                   |
| <b>transport name</b>         | (任意) EAP トランスポートのレジストレーション情報を表示します。              |
| <b>sessions</b>               | EAP セッション情報を表示します。                               |
| <b>credentials name</b>       | (任意) EAP 方式のレジストレーション情報を表示します。                   |
| <b>interface interface-id</b> | (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 EAP 情報を表示します。 |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

次のキーワードとともに **show eap registrations** 特権 EXEC コマンドを使用する場合、コマンド出力には次の情報が表示されます。

- **None** : EAP および登録された EAP 方式で使用されるすべての下位レベル
- **method name** キーワード : 登録された指定の方式
- **transport name** キーワード : 登録された特定の下位レベル

次のキーワードを含む **show eap sessions** 特権 EXEC コマンドを使用する場合、コマンド出力には次の情報が表示されます。

- **None** : すべてのアクティブな EAP セッション
- **credentials name** キーワード : 指定された資格情報プロファイル
- **interface interface-id** キーワード : 指定されたインターフェイスのパラメータ
- **method name** キーワード : 指定された EAP 方式
- **transport name** キーワード : 指定された下位レイヤ

## 例

次の例では、**show eap registrations** すべての特権 EXEC コマンドの出力を示します。

```
Switch> show eap registrations
Registered EAP Methods:
```

```

Method Type Name
4 Peer MD5

Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
1 Authenticator MAB

```

次の例では、**show eap registrations transport** 特権 EXEC コマンドの出力を示します。

```

Switch> show eap registrations transport all
Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
1 Authenticator MAB

```

次の例では、**show eap sessions** 特権 EXEC コマンドの出力を示します。

```

Switch> show eap sessions
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticataInterface: Gi1/1
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None

Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticataInterface: Gi1/2
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0xA800000B Credentials profile: None
Lower layer context ID: 0x0D000005 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None

```

<Output truncated>

次の例では、**show eap sessions interface interface-id** 特権 EXEC コマンドの出力を示します。

```

Switch# show eap sessions interface gigabitethernet1/1
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticataInterface: Gi1/1
Current method: None Method state: Uninitialised
Retransmission count: 1 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None

```

## 関連コマンド

| コマンド                      | 説明                                    |
|---------------------------|---------------------------------------|
| <b>clear eap sessions</b> | スイッチまたは指定されたポートの EAP のセッション情報をクリアします。 |

# show env

スイッチ環境情報を表示するには、EXEC モードで **show env** コマンドを使用します。

```
show env {all | power | temperature [status]}
```

| 構文の説明 | all                | ファンと温度環境ステータスの両方が表示されます。 |
|-------|--------------------|--------------------------|
|       | <b>power</b>       | スイッチの電源状態を表示します。         |
|       | <b>temperature</b> | スイッチの温度ステータスを表示します。      |
|       | <b>status</b>      | (任意) スイッチの内部温度を表示します。    |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

使用上のガイドライン コマンド出力では、GREEN および YELLOW ステートを OK と表示し、RED ステートを FAULTY と表示します。

このスイッチに **show env all** コマンドを入力する場合、コマンド出力は **show env temperature status** コマンド出力と同じです。

しきい値レベルに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーションガイドを参照してください。

例 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: 48 Degree Celsius
POWER SUPPLY A is DC OK
POWER SUPPLY B is DC OK
```

次の例では、**show env power** コマンドの出力を示します。

```
Switch> show env power
Power supply A is DC OK
Power supply B is DC FAULTY
```

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
```

次の例では、**show env temperature status** コマンドの出力を示します。

```
Switch> show env temperature status
Temperature Value: 48 Degree Celsius
```

# show env alarm-contact

アラーム接点の情報を表示するには、EXEC モードで、**show env alarm contact** コマンドを使用します。

**show env alarm contact**

## 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

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、**show env alarm-contact** コマンド出力を示します。

```
Switch# show env alarm-contact
ALARM CONTACT 1
  Status:      not asserted
  Description: line
  Severity:    minor
  Trigger:     closed
ALARM CONTACT 2
  Status:      not asserted
  Description: external alarm contact 2
  Severity:    minor
  Trigger:     closed
Switch#
```

## 関連コマンド

| コマンド                          | 説明                   |
|-------------------------------|----------------------|
| <a href="#">alarm contact</a> | システム アラーム接点の設定を行います。 |

# show errdisable detect

errdisable 検出ステータスを表示するには、EXEC モードで **show errdisable detect** コマンドを使用します。

## show errdisable detect

### 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

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

表示された gbic-invalid エラーの理由は、無効な Small Form-Factor Pluggable (SFP) モジュールを意味します。

### 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
bpdguard             Enabled     vlan
channel-misconfig    Enabled     port
community-limit     Enabled     port
dhcp-rate-limit      Enabled     port
dtp-flap             Enabled     port
gbic-invalid         Enabled     port
inline-power         Enabled     port
invalid-policy       Enabled     port
l2ptguard            Enabled     port
link-flap            Enabled     port
loopback             Enabled     port
lsgroup              Enabled     port
pagp-flap            Enabled     port
psecure-violation    Enabled     port/vlan
security-violatio    Enabled     port
sfp-config-mismat    Enabled     port
storm-control        Enabled     port
udld                  Enabled     port
vmps                  Enabled     port
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">errdisable detect cause</a>     | 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。            |
| <a href="#">show errdisable flap-values</a> | 認識されている状態のエラー情報を表示します。                                  |
| <a href="#">show errdisable recovery</a>    | errdisable 回復タイマーの情報を表示します。                             |
| <a href="#">show interfaces status</a>      | 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、EXEC モードで **show errdisable flap-values** コマンドを使用します。

## show errdisable flap-values

### 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

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

このコマンドの 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 つのダイナミック トランキング プロトコル (DTP) ステート (ポート モード アクセス/トランク)、またはポート集約プロトコル (PAgP) フラップが 30 秒間隔で変更された場合、または 5 つのリンク ステート (リンク アップ/ダウン) が 10 秒間隔で変更された場合は、エラーと見なされてポートがシャットダウンすることが示されます。

```
ErrDisable Reason      Flaps      Time (sec)
-----
pagp-flap              3          30
dtp-flap               3          30
link-flap              5          10
```

### 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  |
|--|---|
| <a href="#">errdisable detect cause</a>  | 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。            |
| <a href="#">show errdisable detect</a>   | errdisable 検出ステータスを表示します。                               |
| <a href="#">show errdisable recovery</a> | errdisable 回復タイマーの情報を表示します。                             |
| <a href="#">show interfaces status</a>   | 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、EXEC モードで **show errdisable recovery** コマンドを使用します。

## show errdisable 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

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

このコマンドの出力に表示される **gbic-invalid error-disable** の理由は、無効な Small Form-Factor Pluggable (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
link-flap             Enabled
l2ptguard             Disabled
psecure-violation    Disabled
gbic-invalid          Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback              Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
-----
Gi1/2        link-flap             279
```

## ■ show errdisable recovery



(注) unicast-flood フィールドは、出力に表示はされますが無効です。

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">errdisable recovery</a>         | 回復メカニズム変数を設定します。  |
| <a href="#">show errdisable detect</a>      | errdisable 検出ステータスを表示します。                               |
| <a href="#">show errdisable flap-values</a> | 認識されている状態のエラー情報を表示します。                                  |
| <a href="#">show interfaces status</a>      | 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、EXEC モードで **show etherchannel** 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}
```

## 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 ~ 6 です。   |
| <b>detail</b>               | 詳細な EtherChannel 情報を表示します。                |
| <b>load-balance</b>         | 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。 |
| <b>port</b>                 | EtherChannel ポートの情報を表示します。                |
| <b>port-channel</b>         | ポート チャンネル情報を表示します。                        |
| <b>protocol</b>             | EtherChannel で使用されるプロトコルを表示します。           |
| <b>summary</b>              | 各チャンネル グループのサマリーを 1 行で表示します。              |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

*channel-group-number* 値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。

## 例

次の例では、**show etherchannel 1 detail** コマンドの出力を示します。

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:  LACP
           Ports in the group:
           -----
Port: Gi1/1
-----

Port state      = Up Mstr In-Bndl
Channel group   = 1           Mode = Active           Gcchange = -
Port-channel    = Po1         GC      = -           Pseudo port-channel = Po1
Port index      = 0           Load = 0x00         Protocol =  LACP
```

## show etherchannel

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<br>Priority | Admin<br>Key | Oper<br>Key | Port<br>Number | Port<br>State |
|-------|-------|-------|-----------------------|--------------|-------------|----------------|---------------|
| Gil/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   | Gil/1 | Active   | 0          |
| 0     | 00   | Gil/2 | Active   | 0          |

Time since last port bundled:    01d:20h:20m:20s    Gil/2

次の例では、**show etherchannel 1 summary** コマンドの出力を示します。

```
Switch> show etherchannel 1 summary
Flags: D - down                    P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3            S - Layer2
       u - unsuitable for bundling
       U - in use            f - failed to allocate aggregator
       d - default port
```

Number of channel-groups in use: 1  
 Number of aggregators:            1

| Group | Port-channel | Protocol | Ports                |
|-------|--------------|----------|----------------------|
| 1     | Po1(SU)      | LACP     | Gil/1(P)    Gil/2(P) |

次の例では、**show etherchannel 1 port-channel** コマンドの出力を示します。

```
Switch> show etherchannel 1 port-channel
Port-channels in the group:
-----
Port-channel: Po1    (Primary Aggregator)
-----

Age of the Port-channel    = 01d:20h:24m:50s
Logical slot/port        = 10/1                    Number of ports = 2
HotStandBy port = null
Port state                = Port-channel Ag-Inuse
Protocol                  = LACP
```

```

Ports in the Port-channel:

Index   Load   Port      EC state   No of bits
-----+-----+-----+-----+-----
0       00     Gi1/1     Active     0
0       00     Gi1/2     Active     0

Time since last port bundled:  01d:20h:24m:44s   Gi1/2

```

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                                   |
|--|--------------------------------------|
| <a href="#">channel-group</a>          | EtherChannel グループにイーサネット ポートを割り当てます。 |
| <a href="#">channel-protocol</a>       | 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。 |
| <a href="#">interface port-channel</a> | 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 facility-alarm status

スイッチに生成されたすべてのアラームを表示するには、EXEC モードで **show facility-alarm status** コマンドを使用します。

**show facility-alarm status [critical | info | major | minor]**

| 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。  |
|       | minor    | (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。  |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

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
toyota_S16_sps1 MAJOR     1 Temp above max primary thresh         MAJ      Oct 06
                Syslog    Disabled

Switch> show facility-alarm status
Source          Severity  Description                               Relay    Time
FastEthernet1/3 MINOR     2 Port Not Forwarding                   NONE     Mar 01
1993 00:02:22
```

| 関連コマンド | コマンド  | 説明  |
|--------|---|---|
|        | <a href="#">alarm facility power-supply</a>       | 電源アラーム オプションを設定します。   |
|        | <a href="#">alarm facility temperature</a>        | 温度アラーム オプションを設定します。   |
|        | <a href="#">alarm profile (グローバル コンフィギュレーション)</a> | 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 fallback profile

スイッチで設定されたフォールバック プロファイルを表示するには、特権 EXEC モードで **show fallback profile** コマンドを使用します。

## show fallback profile

### 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

なし

### コマンド モード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

スイッチで設定されたプロファイルを表示するには、**show fallback profile** 特権 EXEC コマンドを使用します。

### 例

次の例では、**show fallback profile** コマンドの出力を示します。

```
switch# show fallback profile
Profile Name: dot1x-www
-----
Description      : NONE
IP Admission Rule : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
-----
Description      : NONE
IP Admission Rule : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
-----
Description      : NONE
IP Admission Rule : NONE
IP Access-Group IN: NONE
```

### 関連コマンド

| コマンド                             | 説明   |
|----------------------------------|--|
| <a href="#">dot1x fallback</a>   | 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。 |
| <a href="#">fallback profile</a> | Web 認証のフォールバック プロファイルを作成します。                                       |
| <a href="#">ip admission</a>     | スイッチ ポートで Web 認証をイネーブルにします。  |

## ■ show fallback profile

| コマンド   | 説明                               |
|--|----------------------------------|
| <code>ip admission name proxy http</code>        | スイッチで Web 認証をグローバルにイネーブルにします。    |
| <code>show dot1x [interface interface-id]</code> | 指定されたポートの IEEE 802.1x の状態を表示します。 |

# 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 レートの設定を表示するには、EXEC モードで **show fcs-threshold** コマンドを使用します。

## show fcs-threshold

### 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

なし

### コマンド モード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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。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。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。

### 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
```

## ■ show fcs-threshold

## 関連コマンド

| コマンド                          | 説明                        |
|-------------------------------|---------------------------|
| <a href="#">fcs-threshold</a> | 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、EXEC モードで **show flowcontrol** コマンドを使用します。

**show flowcontrol** [*interface interface-id* | *module number*]

|              |                               |  |
|--------------|-------------------------------|--|
| <b>構文の説明</b> | <b>interface interface-id</b> | (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。  |
|              | <b>module number</b>          | (任意) スイッチ上のすべてのインターフェイスのフロー制御ステータスと統計情報を表示します。モジュール番号は 1 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。 |

**デフォルト** なし

**コマンドモード** EXEC

|               |             |                 |
|---------------|-------------|-----------------|
| <b>コマンド履歴</b> | <b>リリース</b> | <b>変更内容</b>     |
|               | 15.0(1)EY   | このコマンドが導入されました。 |

**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。

**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
-----
Gi1/1         Unsupp.  Unsupp.  off      off      0        0
Gi1/2         desired  off      off      off      0        0
Gi1/3         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 gigabitethernet1/2
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
              admin    oper      admin    oper
-----
Gi1/2         desired  off      off      off      0        0
```

## ■ show flowcontrol

## 関連コマンド

| コマンド                        | 説明                          |
|-----------------------------|-----------------------------|
| <a href="#">flowcontrol</a> | インターフェイスの受信フロー制御ステートを設定します。 |

# show interfaces

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管理ステータスおよび動作ステータスを表示するには、特権 EXEC モードで **show interfaces** 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 | rep | pruning | stats | status [err-disabled] |
| backup | module number] | transceiver | properties | detail [module number] | trunk]
```

## 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 チャンネルなどです。ポート チャンネルの範囲は 1 ~ 6 です。   |
| <i>vlan vlan-id</i>  | (任意) VLAN ID を指定します。指定できる範囲は 1 ~ 4094 です。  |
| <b>accounting</b>    | (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。<br><br>(注) ソフトウェアで処理された packets だけが表示されます。ハードウェアでスイッチングされる packets は表示されません。 |
| <b>capabilities</b>  | (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機能 (インターフェイス上で設定可能な機能やオプションを含む) 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またはトランシーバの特性 (上記のキーワードに対応) を表示します。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 を入力するときは利用できません。                        |
| <b>counters</b>      | (任意) 情報 <b>show interfaces counters</b> を表示します。  |
| <b>description</b>   | (任意) 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。   |
| <b>etherchannel</b>  | (任意) インターフェイス EtherChannel 情報を表示します。   |
| <b>flowcontrol</b>   | (任意) インターフェイスのフロー制御情報を表示します。   |
| <b>pruning</b>       | (任意) インターフェイス トランク VTP プルーニング情報を表示します。   |
| <b>rep</b>           | (任意) 情報 <b>show interfaces rep</b> を表示します。   |
| <b>stats</b>         | (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 packets を表示します。  |
| <b>status</b>        | (任意) インターフェイスの状態を表示します。Type フィールドの <b>unsupported</b> のステータスは、他社製の Small Form-Factor Pluggable (SFP) モジュールがモジュール スロットに装着されていることを示しています。        |
| <b>err-disabled</b>  | (任意) <b>errdisable</b> ステートのインターフェイスを表示します。  |
| <b>backup</b>        | (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。   |

|                                      |  |
|--------------------------------------|--|
| <b>transceiver detail properties</b> | (任意) CWDM または DWDM Small Form-Factor Pluggable (SFP) モジュール インターフェイスの物理プロパティを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>detail</b> : (任意) 高低の番号、アラーム情報を含む較正プロパティを表示します。</li> <li><b>properties</b> : (任意) インターフェイスの速度とデュプレックスの設定を表示します。</li> </ul> |
| <b>trunk</b>                         | 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。  |

**デフォルト** なし

**コマンド モード** 特権 EXEC

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

**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。

- スイッチ上の全インターフェイスの機能を表示するには、**show interfaces capabilities module1** コマンドを使用します。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)。



**(注)** **crb**、**fair-queue**、**irb**、**mac-accounting**、**precedence**、**random-detect**、**rate-limit**、および **shape** キーワードは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません。

**例** これは、インターフェイスの **show interfaces interface-id** コマンドの出力例を示します。

```
Switch# show interface GigabitEthernet1/2
GigabitEthernet1/2 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 001e.1300.4882 (bia 001e.1300.4882)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 100Mb/s, link type is auto, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:00, output hang never
  Last clearing of 'show interface' counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```

Output queue: 0/40 (size/max)
5 minute input rate 2000 bits/sec, 4 packets/sec
5 minute output rate 17000 bits/sec, 27 packets/sec
 553226 packets input, 39772509 bytes, 0 no buffer
  Received 530934 broadcasts (529980 multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 529980 multicast, 0 pause input
  0 input packets with dribble condition detected
4031941 packets output, 317450903 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 PAUSE output
  0 output buffer failures, 0 output buffers swapped out

```

次の例では、**show interfaces accounting** コマンドの出力を示します。

```

Switch# show interfaces accounting
Vlan1
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
      IP        1094395   131900022   559555     84077157
      Spanning Tree  283896   17033760    42         2520
      ARP        63738    3825680    231        13860
Interface Vlan2 is disabled
Vlan7
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
Vlan31
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

GigabitEthernet1/1
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/2
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

<output truncated>

```

これは、インターフェイスの **show interfaces capabilities interface-id** コマンドの出力例を示します。

```

Switch# show interfaces GigabitEthernet1/2 capabilities
GigabitEthernet1/2
Model:                IE-3000-4TC
Type:                 Not Present
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-(4q3t) (3t: Two configurable values and one fixed.)
CoS rewrite:          yes
ToS rewrite:          yes
UDLD:                 yes
Inline power:         no
SPAN:                 source/destination
PortSecure:           yes
Dot1x:                yes

```

## show interfaces

```
Multiple Media Types: rj45, sfp, auto-select
```

次の例では、**description** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを **Connects to Marketing** として指定した場合の **show interfaces interface description** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/2 description
Interface Status          Protocol Description
Gi1/2          up                down      Connects to Marketing
```

次の例では、スイッチにポート チャネルが設定されている場合の **show interfaces etherchannel** コマンドの出力を示します。

```
Switch# show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/1          Number of ports = 0
GC                       = 0x00000000      HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/2          Number of ports = 0
GC                       = 0x00000000      HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/3          Number of ports = 0
GC                       = 0x00000000      HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse
```

次の例では、VTP ドメイン内でプルーンングがイネーブルの場合の **show interfaces interface-id pruning** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/2     3,4

Port      Vlans traffic requested of neighbor
Gi1/2     1-3
```

次の例では、指定した VLAN インターフェイスの **show interfaces stats** コマンドの出力を示します。

```
Switch# show interfaces vlan 1 stats
Switching path  Pkts In  Chars In  Pkts Out  Chars Out
Processor      1165354  136205310  570800    91731594
Route cache    0         0          0         0
Total          1165354  136205310  570800    91731594
```

次の例では、**show interfaces status** コマンドの出力の一部を示します。すべてのインターフェイスのステータスが表示されます。

```
Switch# show interfaces status
Port      Name          Status      Vlan      Duplex  Speed Type
Fa1/1     Fa1/1         notconnect  1         auto    auto  10/100BaseTX
Fa1/2     Fa1/2         notconnect  1         auto    auto  10/100BaseTX
Fa1/3     Fa1/3         notconnect  1         auto    auto  10/100BaseTX
Fa1/4     Fa1/4         notconnect  1         auto    auto  10/100BaseTX
Fa2/1     Fa2/1         notconnect  1         auto    auto  10/100BaseTX
Fa2/2     Fa2/2         notconnect  1         auto    auto  10/100BaseTX
Fa2/3     Fa2/3         notconnect  1         auto    auto  10/100BaseTX
Fa2/4     Fa2/4         notconnect  1         auto    auto  10/100BaseTX
```

```

Fa2/5                notconnect 1          auto auto 10/100BaseTX
Fa2/6                notconnect 1          auto auto 10/100BaseTX
Fa2/7                notconnect 1          auto auto 10/100BaseTX
Fa2/8                notconnect 1          auto auto 10/100BaseTX

```

<output truncated>

次の例では、**show interfaces status err-disabled** コマンドの出力を示します。errdisable ステータスのインターフェイスのステータスを表示します。

```

Switch# show interfaces status err-disabled
Port      Name              Status      Reason
Gi1/2                    err-disabled dtp-flap

```

次の例では、**show interfaces interface-id pruning** コマンドの出力を示します。

```

Switch# show interfaces gigabitethernet1/2 pruning
Port      Vlans pruned for lack of request by neighbor

```

次の例では、**show interfaces interface-id trunk** コマンドの出力を示します。ポートのトランッキング情報が表示されます。

```

Switch# show interfaces gigabitethernet1/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi1/1     auto     negotiate      trunking    1

Port      Vlans allowed on trunk
Gi1/1     1-4094

Port      Vlans allowed and active in management domain
Gi1/1     1-4

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/1     1-4

```

次の例では、**show interfaces interface-id transceiver properties** コマンドの出力を示します。

```

Switch# show interfaces gigabitethernet1/2 transceiver properties
Name : Gi1/2
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
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 gigabitethernet1/3 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<br>(Celsius) | High Alarm<br>Threshold<br>(Celsius) | High Warn<br>Threshold<br>(Celsius) | Low Warn<br>Threshold<br>(Celsius) | Low Alarm<br>Threshold<br>(Celsius) |
|-------|--------------------------|--------------------------------------|-------------------------------------|------------------------------------|-------------------------------------|
| Gi1/3 | 41.5                     | 110.0                                | 103.0                               | -8.0                               | -12.0                               |

| Port  | Voltage<br>(Volts) | High Alarm<br>Threshold<br>(Volts) | High Warn<br>Threshold<br>(Volts) | Low Warn<br>Threshold<br>(Volts) | Low Alarm<br>Threshold<br>(Volts) |
|-------|--------------------|------------------------------------|-----------------------------------|----------------------------------|-----------------------------------|
| Gi1/3 |                    |                                    |                                   |                                  |                                   |

## show interfaces

|       |                                    |                                  |                                 |                                |                                 |
|-------|------------------------------------|----------------------------------|---------------------------------|--------------------------------|---------------------------------|
| ----- | -----                              | -----                            | -----                           | -----                          | -----                           |
| Gi1/3 | 3.20                               | 4.00                             | 3.70                            | 3.00                           | 2.95                            |
| Port  | Current<br>(milliamperes)          | High Alarm<br>Threshold<br>(mA)  | High Warn<br>Threshold<br>(mA)  | Low Warn<br>Threshold<br>(mA)  | Low Alarm<br>Threshold<br>(mA)  |
| ----- | -----                              | -----                            | -----                           | -----                          | -----                           |
| Gi1/3 | 31.0                               | 84.0                             | 70.0                            | 4.0                            | 2.0                             |
| Port  | Optical<br>Transmit Power<br>(dBm) | High Alarm<br>Threshold<br>(dBm) | High Warn<br>Threshold<br>(dBm) | Low Warn<br>Threshold<br>(dBm) | Low Alarm<br>Threshold<br>(dBm) |
| ----- | -----                              | -----                            | -----                           | -----                          | -----                           |
| Gi1/3 | -0.0 ( -0.0)                       | -0.0                             | -0.0                            | -0.0                           | -0.0                            |
| Port  | Optical<br>Receive Power<br>(dBm)  | High Alarm<br>Threshold<br>(dBm) | High Warn<br>Threshold<br>(dBm) | Low Warn<br>Threshold<br>(dBm) | Low Alarm<br>Threshold<br>(dBm) |
| ----- | -----                              | -----                            | -----                           | -----                          | -----                           |
| Gi1/3 | N/A ( -0.0) --                     | -0.0                             | -0.0                            | -0.0                           | -0.0                            |

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">switchport access</a>           | 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。                     |
| <a href="#">switchport backup interface</a> | 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 <b>Flex Link</b> を設定します。         |
| <a href="#">switchport block</a>            | 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。                      |
| <a href="#">switchport mode</a>             | ポートの <b>VLAN</b> メンバーシップ モードを設定します。                                |
| <a href="#">switchport protected</a>        | 同じスイッチの他の保護されたポートからレイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離します。 |
| <a href="#">switchport trunk pruning</a>    | トランキング モードのポートの <b>VLAN</b> プルーニング適格リストを設定します。                     |

# show interfaces counters

スイッチ上または特定のインターフェイスの各カウンタを表示するには、特権 EXEC モードで **show interfaces counters** コマンドを使用します。

```
show interfaces [interface-id | vlan vlan-id] counters [errors | etherchannel | protocol status | trunk]
```

| 構文の説明 | パラメータ                  | 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)。   |
|       | <i>vlan vlan-id</i>    | (任意) VLAN の ID。   |
|       | <b>errors</b>          | (任意) エラー カウンタを表示します。  |
|       | <b>etherchannel</b>    | (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。 |
|       | <b>protocol status</b> | (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。   |
|       | <b>trunk</b>           | (任意) トランク カウンタを表示します。   |

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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

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。



(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。

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を表示します。

```
Switch# show interfaces counters
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi1/1         0           0             0             0
Gi1/2         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
```

## ■ show interfaces counters

```

Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
FastEthernet1/1: Other, IP, ARP, CDP
FastEthernet1/2: Other, IP
FastEthernet1/3: Other, IP
FastEthernet1/4: Other, IP
FastEthernet1/5: Other, IP
FastEthernet1/6: Other, IP
FastEthernet1/7: Other, IP
FastEthernet1/8: Other, IP
FastEthernet1/9: Other, IP
FastEthernet1/10: 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 カウンタを表示します。

```

Switch# show interfaces counters trunk
Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/1         0               0               0
Gi1/2         0               0               0
Gi1/1         80678          4155            0
Gi1/2         82320          126             0

```

<output truncated>

## 関連コマンド

| コマンド                            | 説明                    |
|---------------------------------|-----------------------|
| <a href="#">show interfaces</a> | 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) の設定およびステータスを表示するには、EXEC モードで **show interfaces rep** コマンドを使用します。

**show interfaces** [*interface-id*] **rep** [**detail**]

|       |                     |                                     |
|-------|---------------------|-------------------------------------|
| 構文の説明 | <i>interface-id</i> | (任意) 指定した物理インターフェイスまたはポート チャンネル ID。 |
|       | <b>detail</b>       | (任意) 詳細な REP 設定およびステータス情報を表示します。    |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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。

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 1/1      1       Primary Edge  TWO_WAY  Open
GigabitEthernet 1/2      1       Edge          TWO_WAY  Open
FastEthernet 1/4    2                     INIT_DOWN Fail
```

## show interfaces rep

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
-----
GigabitEthernet1/1  2          TWO_WAY      Open
GigabitEthernet1/2  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
-----
GigabitEthernet1/1  1          NO_NEIGHBOR  FailNoNbr
GigabitEthernet1/2  2          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 gigabitethernet1/2 rep detail
GigabitEthernet1/2  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  |
|--|---|
| <a href="#">rep segment</a>                | 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。 |
| <a href="#">show rep topology [detail]</a> | 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 inventory

ハードウェアの製品識別 (PID) 情報を表示するには、EXEC モードで **show inventory** コマンドを使用します。

**show inventory** [*entity-name* | **raw**]

| 構文の説明 | <i>entity-name</i> | (任意) 指定されたエンティティ。たとえば、Small Form-Factor Pluggable (SFP) モジュールが取り付けられているインターフェイス (gigabitethernet1/1 など) を入力します。 |
|-------|--------------------|---|
|       | <b>raw</b>         | (任意) デバイスのすべてのエンティティを表示します。   |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

使用上のガイドライン  
 コマンドでは大文字と小文字が区別されます。引数がない場合、**show inventory** コマンドは製品識別情報を持つすべての識別可能なエンティティのコンパクト ダンプを生成します。コンパクト ダンプには、エンティティの場所 (スロット ID)、エンティティの説明、およびそのエンティティの Unique Device Indicator (UDI) (PID、VID、および SN) が表示されます。



(注) PID がない場合は、**show inventory** コマンドを入力しても出力は表示されません。

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: 'IE-3000-4TC'
PID: IE-3000-4TC      , VID:      , SN: FHK1152UZRW

NAME: 'IE-3000-4TC - Module in slot 1', DESCR: 'IE-3000-4TC - Module in slot 1'
PID: 800-28491-01, VID: C1151V545FOC11504, SN: S9FOC115040MRFOC11503J7JF

NAME: 'IEM-3000-8TM - Module in slot 2', DESCR: 'IEM-3000-8TM - Module in slot 2'
PID: 800-28540-01, VID: C1151V332FOC11515, SN: P0FOC11504ML3

NAME: 'IEM-3000-8FM - Module in slot 3', DESCR: 'IEM-3000-8FM - Module in slot 3'
PID: 800-28543-01, VID: C1151V462FOC11505, SN: GTFOC11505JMPFOC11505JDX

Switch>
```

# show ip arp inspection

ダイナミック アドレス解決プロトコル (ARP) インспекションの設定および動作ステート、あるいはすべての VLAN または指定されたインターフェイスや VLAN に対するこの機能のステータスを表示するには、特権 EXEC モードで **show ip arp inspection** 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]
```

## 構文の説明

|                                |   |
|--------------------------------|---|
| <b>interfaces interface-id</b> | (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。   |
| <b>log</b>                     | (任意) ダイナミック ARP インспекション ログ バッファの設定と内容を表示します。  |
| <b>statistics</b>              | (任意) 指定された VLAN の転送済みパケット、ドロップ済みパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、アクセス コントロール リスト (ACL) によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекション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。                    |
| <b>vlan vlan-range</b>         | (任意) 指定された VLAN のダイナミック ARP インспекションの設定および動作ステートを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекション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。<br><br>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

なし

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、**show ip arp inspection** コマンドの出力を示します。

```
Switch# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

Vlan      Configuration  Operation  ACL Match  Static ACL
```

```

-----
 1      Enabled      Active      deny-all      No
-----
Vlan    ACL Logging      DHCP Logging      Probe Logging
-----
 1      Acl-Match      All              Permit
-----
Vlan    Forwarded      Dropped      DHCP Drops      ACL Drops
-----
 1              0              0              0              0
-----
Vlan    DHCP Permits      ACL Permits      Probe Permits      Source MAC Failures
-----
 1              0              0              0              0
-----
Vlan    Dest MAC Failures      IP Validation Failures      Invalid Protocol Data
-----
 1              0              0              0

```

次の例では、**show ip arp inspection interfaces** コマンドの出力を示します。

```

Switch# show ip arp inspection interfaces
-----
Interface      Trust State      Rate (pps)      Burst Interval
-----
Gi1/1          Untrusted        15              1
Gi1/2          Untrusted        15              1
Gi1/3          Untrusted        15              1

```

次の例では、**show ip arp inspection interfaces interface-id** コマンドの出力を示します。

```

Switch# show ip arp inspection interfaces gigabitethernet1/1
-----
Interface      Trust State      Rate (pps)      Burst Interval
-----
Gi1/1          Untrusted        15              1

```

次の例では、**show ip arp inspection log** コマンドの出力を示します。バッファがクリアされる前のログ バッファの内容を表示します。

```

Switch# show ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 10 entries per 300 seconds.
-----
Interface      Vlan      Sender MAC      Sender IP      Num Pkts      Reason      Time
-----
Gi1/1          5         0003.0000.d673  192.2.10.4     5             DHCP Deny   19:39:01 UTC
Mon Mar 1 1993
Gi1/1          5         0001.0000.d774  128.1.9.25     6             DHCP Deny   19:39:02 UTC
Mon Mar 1 1993
Gi1/1          5         0001.c940.1111  10.10.10.1     7             DHCP Deny   19:39:03 UTC
Mon Mar 1 1993
Gi1/1          5         0001.c940.1112  10.10.10.2     8             DHCP Deny   19:39:04 UTC
Mon Mar 1 1993
Gi1/1          5         0001.c940.1114  173.1.1.1      10            DHCP Deny   19:39:06 UTC
Mon Mar 1 1993
Gi1/1          5         0001.c940.1115  173.1.1.2      11            DHCP Deny   19:39:07 UTC
Mon Mar 1 1993
Gi1/1          5         0001.c940.1116  173.1.1.3      12            DHCP Deny   19:39:08 UTC
Mon Mar 1 1993

```

ログ バッファでオーバーフローが生じた場合は、1つのログ イベントがログ バッファ内に収まらなかったことを意味し、**show ip arp inspection log** 特権 EXEC コマンドによる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。このエントリに対しては、

## show ip arp inspection

その他の統計情報は表示されません。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 インスペクション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 インスペクション 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。VLAN 5 のダイナミック ARP によって処理された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 インスペクション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                                    |
|--|---------------------------------------|
| <a href="#">arp access-list</a>                    | ARP ACL を定義します。                       |
| <a href="#">clear arp inspection log</a>           | ダイナミック ARP インспекション ログ バッファをクリアします。  |
| <a href="#">clear ip arp inspection statistics</a> | ダイナミック ARP インспекションの統計情報をクリアします。     |
| <a href="#">ip arp inspection log-buffer</a>       | ダイナミック ARP インспекション ロギング バッファを設定します。 |
| <a href="#">ip arp inspection vlan logging</a>     | VLAN 単位で記録するパケットのタイプを制御します。           |
| <a href="#">show arp access-list</a>               | 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、EXEC モードで **show ip dhcp snooping** コマンドを使用します。

## show 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

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

このコマンドは、グローバル コンフィギュレーションの結果だけを表示します。したがって、この例では、ストリングがサーキット ID 用に設定されていた場合も、サーキット ID サブオプションは **vlan-mod-port** のデフォルト形式で表示されます。

### 例

次の例では、**show ip dhcp snooping** コマンドの出力を示します。

```
Switch> show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
circuit-id format: vlan-mod-port
    remote-id format: string
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----                -
GigabitEthernet1/1      yes          unlimited
GigabitEthernet1/2      yes          unlimited
```

### 関連コマンド

| コマンド  | 説明                           |
|---|------------------------------|
| <a href="#">show ip dhcp snooping binding</a> | 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

スイッチ上の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 データベースおよび設定情報を表示するには、スイッチに、EXEC モードで **show ip dhcp snooping binding** 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*]

## 構文の説明

|                                      |                              |
|--------------------------------------|------------------------------|
| <i>ip-address</i>                    | (任意) バインディング エントリの IP アドレス。  |
| <i>mac-address</i>                   | (任意) バインディング エントリの MAC アドレス。 |
| <b>interface</b> <i>interface-id</i> | (任意) バインディング入力インターフェイス。      |
| <b>vlan</b> <i>vlan-id</i>           | (任意) バインディング エントリ VLAN。      |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 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    GigabitEthernet1/1
00:D0:B7:1B:35:DE  10.1.2.151        237        dhcp-snooping  20    GigabitEthernet1/2
Total number of bindings: 2
```

次の例では、特定の IP アドレスの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding 10.1.2.150
-----
MacAddress          IpAddress          Lease(sec)  Type           VLAN  Interface
-----
01:02:03:04:05:06  10.1.2.150        9810       dhcp-snooping  20    GigabitEthernet1/1
Total number of bindings: 1
```

## ■ show ip dhcp snooping binding

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   GigabitEthernet1/2
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 gigabitethernet1/2
-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN  Interface
-----
00:30:94:C2:EF:35  10.1.2.151    290           dhcp-snooping  20   GigabitEthernet1/2
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   GigabitEthernet1/1
00:00:00:00:00:02  10.1.2.151    65            dhcp-snooping  20   GigabitEthernet1/2
Total number of bindings: 2
```

表 2-26 では、show ip dhcp snooping binding コマンドの出力結果における各フィールドについて説明します。

表 2-26 show ip dhcp snooping binding コマンドの出力結果

| 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 サーバから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<br>(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                                |
|--|-----------------------------------|
| <a href="#">ip dhcp snooping binding</a> | 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。 |
| <a href="#">show ip dhcp snooping</a>    | 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、EXEC モードで **show ip dhcp snooping database** コマンドを使用します。

## show ip dhcp snooping database [detail]

| 構文の説明     | <b>detail</b> (任意) 詳細なステータスおよび統計情報を表示します。   |      |      |           |                 |
|-----------|---|------|------|-----------|-----------------|
| デフォルト     | なし  |      |      |           |                 |
| コマンドモード   | EXEC  |      |      |           |                 |
| コマンド履歴    | <table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>15.0(1)EY</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 15.0(1)EY | このコマンドが導入されました。 |
| リリース      | 変更内容  |      |      |           |                 |
| 15.0(1)EY | このコマンドが導入されました。   |      |      |           |                 |

**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

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
```

## ■ show ip dhcp snooping database

```

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  |
|---|---|
| <a href="#">ip dhcp snooping</a>          | VLAN 上で DHCP スヌーピングをイネーブルにします。                          |
| <a href="#">ip dhcp snooping database</a> | 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。 |
| <a href="#">show ip dhcp snooping</a>     | DHCP スヌーピング情報を表示します。                                    |

# show ip dhcp snooping statistics

DHCP スヌーピングの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、EXEC モードで **show ip dhcp snooping statistics** コマンドを使用します。

## show ip dhcp snooping statistics [detail]

| 構文の説明     | <b>detail</b> (任意) 表示詳細な統計情報を表示します。   |      |      |           |                 |
|-----------|---|------|------|-----------|-----------------|
| デフォルト     | なし  |      |      |           |                 |
| コマンドモード   | EXEC  |      |      |           |                 |
| コマンド履歴    | <table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>15.0(1)EY</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 15.0(1)EY | このコマンドが導入されました。 |
| リリース      | 変更内容  |      |      |           |                 |
| 15.0(1)EY | このコマンドが導入されました。   |      |      |           |                 |

**使用上のガイドライン** スイッチ スタックでは、すべての統計情報がスタック マスターで生成されます。新しいスタック マスターが選出された場合、統計カウンタはリセットされます。

**例** 次の例では、**show ip dhcp snooping statistics** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics
Packets Forwarded                = 0
Packets Dropped                   = 0
Packets Dropped From untrusted ports = 0
```

次の例では、**show ip dhcp snooping statistics detail** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics detail
Packets Processed by DHCP Snooping = 0
Packets Dropped Because
  IDB not known                    = 0
  Queue full                        = 0
  Interface is in errdisabled       = 0
  Rate limit exceeded               = 0
  Received on untrusted ports      = 0
  Nonzero giaddr                   = 0
  Source mac not equal to chaddr    = 0
  Binding mismatch                  = 0
  Insertion of opt82 fail           = 0
  Interface Down                    = 0
  Unknown output interface          = 0
  Reply output port equal to input port = 0
  Packet denied by platform         = 0
```

```
show ip dhcp snooping statistics
```

表 2-27 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 2-27 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 <b>no ip dhcp snooping information option allow-untrusted</b> 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、 <b>ip dhcp snooping verify mac-address</b> グローバル コンフィギュレーション コマンドが設定されている回数。   |
| Binding mismatch                      | MAC アドレスと VLAN のペアのバインディングになっているポートとは異なるポートで、RELEASE パケットまたは DECLINE パケットを受信した回数。これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがスイッチの別のポートに移動して RELEASE または DECLINE を実行したことを表すこともあります。MAC アドレスは、イーサネット ヘッダーの送信元 MAC アドレスではなく、DHCP パケットの chaddr フィールドから採用されます。 |
| Insertion of opt82 fail               | パケットへのオプション 82 挿入がエラーになった回数。オプション 82 データを含むパケットがインターネットの単一物理パケットのサイズを超えた場合、挿入はエラーになることがあります。   |
| Interface Down                        | パケットが DHCP リレー エージェントへの応答であるが、リレー エージェントの SVI インターフェイスがダウンしている回数。DHCP サーバへのクライアント要求の送信と応答の受信の間で SVI がダウンした場合に発生するエラーですが、めったに発生しません。  |
| Unknown output interface              | オプション 82 データまたは MAC アドレス テーブルのルックアップのいずれかで、DHCP 応答パケットの出力インターフェイスを判断できなかった回数。パケットはドロップされます。オプション 82 が使用されておらず、クライアント MAC アドレスが期限切れになった場合に発生することがあります。ポートセキュリティ オプションで IPSG がイネーブルであり、オプション 82 がイネーブルでない場合、クライアントの MAC アドレスは学習されず、応答パケットはドロップされます。                    |

表 2-27 DHCP スヌーピング統計情報 (続き)

| DHCP スヌーピング統計情報                       | 説明   |
|---------------------------------------|--|
| Reply output port equal to input port | DHCP 応答パケットの出力ポートが入力ポートと同じであり、ループの可能性の原因となった回数。ネットワークの設定の誤り、またはポートの信頼設定の誤用の可能性を示します。 |
| Packet denied by platform             | プラットフォーム固有のレジストリによってパケットが拒否された回数。  |

| 関連コマンド | コマンド                                   | 説明  |
|--------|--|---|
|        | <a href="#">clear ip dhcp snooping</a> | 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)、または指定された IGMP プロファイルを表示するには、特権 EXEC モードで **show ip igmp profile** コマンドを使用します。

**show ip igmp profile** [*profile number*]

|       |                       |   |
|-------|-----------------------|---|
| 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。 |
|-------|-----------------------|---|

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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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                         |
|--------|---------------------------------|----------------------------|
|        | <a href="#">ip igmp profile</a> | 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) スヌーピングの設定を表示するには、**show ip igmp snooping EXEC** コマンドを使用します。

**show ip igmp snooping [groups | mrouter | querier] [vlan *vlan-id*]**

|       |                            |  |
|-------|----------------------------|--|
| 構文の説明 | <b>groups</b>              | (任意) <b>show ip igmp snooping groups</b> 情報を表示します。                       |
|       | <b>mrouter</b>             | (任意) <b>show ip igmp snooping mrouter</b> 情報を表示します。                      |
|       | <b>querier</b>             | (任意) <b>show ip igmp snooping querier</b> 情報を表示します。                      |
|       | <b>vlan <i>vlan-id</i></b> | (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)。 |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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。

**例** 次の例では、**show ip igmp snooping vlan 1** コマンドの出力を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----
IGMP snooping                :Enabled
IGMPv3 snooping (minimal)    :Enabled
Report suppression           :Enabled
TCN solicit query            :Disabled
TCN flood query count        :2
Last member query interval   : 100

Vlan 1:
-----
IGMP snooping                :Enabled
Immediate leave               :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode    :IGMP_ONLY
Last member query interval   : 100
```

## ■ show ip igmp snooping

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  |
|---|---|
| <a href="#">ip igmp snooping</a>                            | 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。     |
| <a href="#">ip igmp snooping last-member-query-interval</a> | IGMP スヌーピングの設定可能な Leave タイマーをイネーブルにします。   |
| <a href="#">ip igmp snooping querier</a>                    | レイヤ 2 ネットワークの IGMP クエリア機能をイネーブルにします。      |
| <a href="#">ip igmp snooping report-suppression</a>         | IGMP レポート抑制をイネーブルにします。                    |
| <a href="#">ip igmp snooping tcn</a>                        | IGMP トポロジ変更通知動作を設定します。                    |
| <a href="#">ip igmp snooping tcn flood</a>                  | IGMP トポロジ変更通知動作としてマルチキャスト フラッディングを指定します。  |
| <a href="#">ip igmp snooping vlan immediate-leave</a>       | VLAN の IGMP スヌーピング即時脱退処理をイネーブルにします。       |
| <a href="#">ip igmp snooping vlan mrouter</a>               | マルチキャスト ルータ ポートを追加、またはマルチキャストの学習方式を設定します。 |
| <a href="#">ip igmp snooping vlan static</a>                | レイヤ 2 ポートをマルチキャスト グループのメンバとして静的に追加します。    |
| <a href="#">show ip igmp snooping groups</a>                | スイッチの IGMP スヌーピング マルチキャスト テーブルを表示します。     |

| コマンド                                       | 説明  |
|--|---|
| <code>show ip igmp snooping mrouter</code> | 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。 |
| <code>show ip igmp snooping querier</code> | 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

スイッチまたはマルチキャスト情報のインターネット グループ管理プロトコル (IGMP) のスヌーピング マルチキャスト テーブルを表示するには、特権 EXEC モードで **show ip igmp snooping groups** 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 [vlan vlan-id [ip\_address] | dynamic | user] [count]**

## 構文の説明

|                     |  |
|---------------------|--|
| <b>vlan vlan-id</b> | (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。 |
| <b>ip_address</b>   | (任意) 指定したグループの IP アドレス。                                |
| <b>dynamic</b>      | (任意) IGMP スヌーピングによって学習されたエントリを表示します。                   |
| <b>user</b>         | (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。                       |
| <b>count</b>        | (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。          |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 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           Gi1/1, Gi1/2
104       224.1.4.3      igmp          v2           Gi1/1, Gi1/2
```

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        Gi1/1, Fa1/8
104       224.1.4.3  igmp     v2        Gi1/1, Fa1/8

```

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        Gi1/1, Fa1/8

```

#### 関連コマンド

| コマンド                                 | 説明  |
|--------------------------------------|---|
| <b>ip igmp snooping</b>              | 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。                         |
| <b>ip igmp snooping vlan mrouter</b> | マルチキャスト ルータ ポートを設定します。  |
| <b>ip igmp snooping vlan static</b>  | レイヤ 2 ポートをマルチキャスト グループのメンバとして静的に追加します。                        |
| <b>show ip igmp snooping</b>         | スイッチまたは VLAN の IGMP スヌーピング設定を表示します。                           |
| <b>show ip igmp snooping mrouter</b> | スイッチまたは指定されたマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。 |

# show ip igmp snooping mrouter

スイッチまたは指定されたマルチキャスト VLAN のダイナミック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、特権 EXEC モードで **show ip igmp snooping mrouter** コマンドを使用します。

**show ip igmp snooping mrouter [vlan vlan-id]**

|       |                     |  |
|-------|---------------------|--|
| 構文の説明 | <b>vlan vlan-id</b> | (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。 |
|-------|---------------------|--|

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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

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。

マルチキャスト VLAN レジストレーション (MVR) 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。

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      Gil/1(dynamic)
```

| 関連コマンド | コマンド  | 説明  |
|--------|---|---|
|        | <a href="#">ip igmp snooping</a>              | 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。           |
|        | <a href="#">ip igmp snooping vlan mrouter</a> | マルチキャスト ルータ ポートを追加します。                          |
|        | <a href="#">ip igmp snooping vlan static</a>  | レイヤ 2 ポートをマルチキャスト グループのメンバとして静的に追加します。          |
|        | <a href="#">show ip igmp snooping</a>         | スイッチまたは VLAN の IGMP スヌーピング設定を表示します。             |
|        | <a href="#">show ip igmp snooping groups</a>  | スイッチまたは指定されたパラメータの IGMP スヌーピング マルチキャスト情報を表示します。 |

# show ip igmp snooping querier

スイッチで設定された IGMP クエリアの設定および動作情報を表示するには、EXEC モードで **show ip igmp snooping querier detail** コマンドを使用します。

```
show ip igmp snooping querier [detail | vlan vlan-id [detail]]
```

| 構文の説明 | detail                            | (任意) 詳細な IGMP クエリア情報を表示します。  |
|-------|-----------------------------------|--|
|       | <b>vlan <i>vlan-id</i> detail</b> | (任意) 指定された VLAN の IGMP クエリア情報を表示します。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。詳細情報を表示するには、 <b>detail</b> キーワードを使用します。 |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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 EXEC** コマンドは、**show ip igmp snooping querier** コマンドに類似しています。ただし、**show ip igmp snooping querier** コマンドでは、スイッチ クエリアにより直前に検出されたデバイス IP アドレスだけが表示されます。

**show ip igmp snooping querier detail** コマンドは、スイッチ クエリアによって最後に検出されたデバイスの IP アドレスのほか、次の追加情報を表示します。

- VLAN で選択されている IGMP クエリア
- VLAN で設定されたスイッチ クエリア (ある場合) に関連する設定および動作情報

**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                 Gil/1
2         172.20.40.20    v2                 Router
```

## ■ show ip igmp snooping querier

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                 Fa1/1
```

```
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 Fa1/1
-----
```

```
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  |
|--|---|
| <a href="#">ip igmp snooping</a>         | 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。                         |
| <a href="#">ip igmp snooping querier</a> | レイヤ 2 ネットワークの IGMP クエリア機能をイネーブルにします。                          |
| <a href="#">show ip igmp snooping</a>    | スイッチまたは指定されたマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。 |

# show ip source binding

スイッチ上の IP ソース バインディングを表示するには、EXEC モードで **show ip source binding** コマンドを使用します。

**show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**interface** *interface-id*] [**vlan** *vlan-id*]

## 構文の説明

|                               |  |
|-------------------------------|--|
| <b>ip-address</b>             | (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。         |
| <b>mac-address</b>            | (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。        |
| <b>dhcp-snooping</b>          | (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。 |
| <b>static</b>                 | (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。               |
| <b>interface interface-id</b> | (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。        |
| <b>vlan vlan-id</b>           | (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。          |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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    GigabitEthernet1/1
00:00:00:0A:00:0A  11.0.0.2      10000      dhcp-snooping  10    GigabitEthernet1/1
```

## 関連コマンド

| コマンド                                     | 説明                                |
|--|-----------------------------------|
| <a href="#">ip dhcp snooping binding</a> | 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。 |
| <a href="#">ip source binding</a>        | スイッチにスタティック IP 送信元バインディングを設定します。  |

# show ip verify source

スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示するには、EXEC モードで **show ip verify source** コマンドを使用します。

**show ip verify source** [*interface interface-id*]

| 構文の説明     | <b>interface interface-id</b> (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。  |      |      |           |                 |
|-----------|---|------|------|-----------|-----------------|
| デフォルト     | なし  |      |      |           |                 |
| コマンドモード   | EXEC  |      |      |           |                 |
| コマンド履歴    | <table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>15.0(1)EY</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 15.0(1)EY | このコマンドが導入されました。 |
| リリース      | 変更内容  |      |      |           |                 |
| 15.0(1)EY | このコマンドが導入されました。   |      |      |           |                 |

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
-----  -
gil1/1    ip             active       10.0.0.1    -----
gil1/1    ip             active       deny-all   11-20
gil1/2    ip             inactive-trust-port
gil1/3    ip             inactive-no-snooping-vlan
gil1/4    ip-mac        active       10.0.0.2    aaaa.bbbb.cccc 10
gil1/4    ip-mac        active       11.0.0.1    aaaa.bbbb.cccd 11
gil1/4    ip-mac        active       deny-all   deny-all       12-20
gil1/5    ip-mac        active       10.0.0.3    permit-all    10
gil1/5    ip-mac        active       deny-all   permit-all     11-20
```

上記の例では、IP 送信元ガードの設定は次のようになります。

- Gigabit Ethernet 1 インターフェイスでは、DHCP スヌーピングは VLAN 10 ~ 20 上でイネーブルです。VLAN 10 では、IP アドレス フィルタリングによる IP ソース ガードがインターフェイスで設定され、バインディングがインターフェイスに存在します。VLAN 11 ~ 20 では、2 番目のエントリが、IP ソース ガードが設定されていない VLAN のインターフェイスで、デフォルト ポートのアクセス コントロール リスト (ACL) が適用されていることを示します。
- Gigabit Ethernet 2 インターフェイスは、信頼性のある DHCP スヌーピングとして設定されています。
- Gigabit Ethernet 3 インターフェイスでは、DHCP スヌーピングは、インターフェイスが所属する VLAN 上でイネーブルではありません。
- Gigabit Ethernet 4 インターフェイスでは、送信元 IP および MAC アドレスのフィルタリングによる IP ソース ガードがイネーブルで、スタティックな IP 送信元バインディングが VLAN 10 と 11 で設定されます。VLAN 12 ~ 20 では、IP ソース ガードが設定されていない VLAN のインターフェイスで、デフォルト ポートの ACL が適用されています。

- Gigabit Ethernet 5 インターフェイスでは、送信元 IP および MAC アドレスのフィルタリングによる IP ソース ガードがイネーブルで、スタティックな IP バインディングで設定されていますが、ポート セキュリティはディセーブルです。スイッチは、送信元 MAC アドレスをフィルタリングできません。

次の例では、IP 送信元ガードがディセーブルにされたインターフェイスの出力を示します。

```
Switch> show ip verify source gigabitethernet 1/6  
IP source guard is not configured on the interface gi1/16.
```

#### 関連コマンド

| コマンド                             | 説明                              |
|----------------------------------|---------------------------------|
| <a href="#">ip verify source</a> | 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) 設定、ステータス、統計情報を表示するには、EXEC モードで **show ipc** をコマンド使用します。

```
show ipc {hog-info | mcast {appclass | groups | status} | nodes | ports [open] | queue | rpc | session
        {all | rx | tx} [verbose] | status [cumlulative] | zones}
```

## 構文の説明

|   |   |
|---|---|
| <b>hog-info</b>                         | 過剰な CPU を消費した IPC メッセージを表示します。  |
| <b>mcast appclass   groups   status</b> | 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"> <li>• <b>appclass</b> : 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。</li> <li>• <b>groups</b> : IPC マルチキャスト グループを表示します。</li> <li>• <b>status</b> : 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。</li> </ul>    |
| <b>nodes</b>                            | 参加ノードを表示します。  |
| <b>ports open</b>                       | 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"> <li>• <b>open</b> : (任意) オープン ポートだけを表示します。</li> </ul>   |
| <b>queue</b>                            | IPC 送信キューの内容を表示します。   |
| <b>rpc</b>                              | IPC リモート プロシージャの統計情報を表示します。   |
| <b>session all   rx   tx</b>            | 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"> <li>• <b>all</b> : セッションの統計情報をすべて表示します。</li> <li>• <b>rx</b> : 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。</li> <li>• <b>tx</b> : 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。</li> </ul> |
| <b>verbose</b>                          | (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)。  |
| <b>status cumlulative</b>               | 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"> <li>• <b>cumlulative</b> : (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。</li> </ul>   |
| <b>zones</b>                            | 参加している IPC ゾーンを表示します。スイッチは 1 つの IPC ゾーンをサポートします。  |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、スイッチが IP サービス イメージを稼働している場合にだけ使用できます。

## 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

Total Frames                Tx          Rx
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.
```

## ■ show ipc

```

Messages currently in use           :           3
Message cache size                 :          1000
Maximum message cache usage        :          1000

0 times message cache crossed      5000 [max]

Emergency messages currently in use :           0

There are 2 messages currently reserved for reply msg.

Inbound message queue depth 0
Zone inbound message queue depth 0

```

次の例では、すべての IPC セッションの統計情報を表示する方法を示します。

```

Switch# show ipc session all
Tx Sessions:
Port ID      Type      Name
10000.7     Unicast   MDFS RP:Statistics
  port_index = 0  type = Unreliable  last sent = 0    last heard = 0
  Msgs requested = 180  Msgs returned = 180

10000.8     Unicast   Slot 1 :MDFS.control.RIL
  port_index = 0  type = Reliable    last sent = 0    last heard = 0
  Msgs requested = 0   Msgs returned = 0

Rx Sessions:
Port ID      Type      Name
10000.7     Unicast   MDFS RP:Statistics
  port_index = 0  seat_id = 0x10000  last sent = 0    last heard = 0
  No of msgs requested = 180  Msgs returned = 180

10000.8     Unicast   Slot 1 :MDFS.control.RIL
  port_index = 0  seat_id = 0x10000  last sent = 0    last heard = 0
  No of msgs requested = 0    Msgs returned = 0

```

次の例では、ローカル IPC サーバのステータスを表示する方法を示します。

```

Switch> show ipc status cumulative
                IPC System Status

Time last IPC stat cleared :never

This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.

1000 IPC Message Headers Cached.

                Rx Side      Tx Side

Total Frames                12916      608
  0                          0
Total from Local Ports      13080      574
Total Protocol Control Frames    116      17
Total Frames Dropped          0          0

                Service Usage

Total via Unreliable Connection-Less Service    12783      171
Total via Unreliable Sequenced Connection-Less Svc    0          0
Total via Reliable Connection-Oriented Service    17          116
<output truncated>

```

## 関連コマンド

| コマンド                      | 説明                              |
|---------------------------|---------------------------------|
| <a href="#">clear ipc</a> | 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 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、特権 EXEC モードで **show ipv6 dhcp conflict** コマンドを使用します。

## show ipv6 dhcp conflict



(注)

このコマンドは、スイッチでデュアル IPv4/IPv6 SDM テンプレートが設定されており、スイッチが IP サービス イメージで実行されている場合にだけ使用可能です。

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

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

競合を検出するように DHCPv6 サーバを設定する場合、DHCPv6 サーバは ping を使用します。クライアントは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  |
|---------------------------------|---|
| <b>clear ipv6 dhcp conflict</b> | 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。                 |
| <b>ipv6 dhcp pool</b>           | 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 mld snooping

スイッチまたは VLAN の IP version 6 (IPv6) マルチキャストリスナー検出 (MLD) スヌーピング設定を表示するには、EXEC モードで **show ipv6 mld snooping** コマンドを使用します。

**show ipv6 mld snooping [vlan *vlan-id*]**

|       |                            |  |
|-------|----------------------------|--|
| 構文の説明 | <b>vlan <i>vlan-id</i></b> | (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。 |
|-------|----------------------------|--|

|       |    |
|-------|----|
| デフォルト | なし |
|-------|----|

|         |      |
|---------|------|
| コマンドモード | EXEC |
|---------|------|

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン**

スイッチまたは特定の VLAN の MLD スヌーピングの設定を表示するのにこのコマンドを使用します。1002 ~ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

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



**(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。

**例**

次の例では、**show ipv6 mld snooping vlan** コマンドの出力を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Switch> show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-----
MLD snooping                : Enabled
MLDv2 snooping (minimal)    : Enabled
Listener message suppression : Enabled
TCN solicit query           : Disabled
TCN flood query count       : 2
Robustness variable         : 3
Last listener query count   : 2
Last listener query interval : 1000
Vlan 100:
-----
MLD snooping                : Disabled
MLDv1 immediate leave       : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable         : 3
```

## ■ show ipv6 mld snooping

```
Last listener query count      : 2
Last listener query interval  : 1000
```

次の例では、**show ipv6 mld snooping** コマンドの出力を示します。ここでは、スイッチ上の VLAN すべてのスヌーピング特性を表示します。

```
Switch> show ipv6 mld snooping
Global MLD Snooping configuration:
-----
MLD snooping                : Enabled
MLDv2 snooping (minimal)    : Enabled
Listener message suppression : Enabled
TCN solicit query          : Disabled
TCN flood query count       : 2
Robustness variable         : 3
Last listener query count   : 2
Last listener query interval : 1000

Vlan 1:
-----
MLD snooping                : Disabled
MLDv1 immediate leave       : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable         : 1
Last listener query count   : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
-----
MLD snooping                : Disabled
MLDv1 immediate leave       : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable         : 3
Last listener query count   : 2
Last listener query interval : 1000
```

## 関連コマンド

| コマンド                              | 説明  |
|-----------------------------------|---|
| <a href="#">ipv6 mld snooping</a> | スイッチ上または VLAN 上の MLD スヌーピングをイネーブルにし、設定を行います。      |
| <a href="#">sdm prefer</a>        | 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に SDM テンプレートを設定します。 |

# show ipv6 mld snooping address

マルチキャストリスナー検出 (MLD) スヌーピングが保持するすべての、または指定された IP version 6 (IPv6) マルチキャストアドレス情報を表示するには、EXEC モードで **show ipv6 mld snooping address** コマンドを使用します。

```
show ipv6 mld snooping address [[vlan vlan-id] [ipv6 multicast-address]] [vlan vlan-id] [count | dynamic | user]
```

| 構文の説明 | パラメータ                         | 説明  |
|-------|-------------------------------|---|
|       | <b>vlan vlan-id</b>           | (任意) MLD スヌーピング マルチキャスト アドレス情報を表示する VLAN を指定します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 |
|       | <b>ipv6-multicast-address</b> | (任意) 指定された IPv6 マルチキャスト アドレスに関する情報を表示します。このキーワードは、VLAN ID を入力した場合だけ使用できます。                      |
|       | <b>count</b>                  | (任意) スイッチ上または指定された VLAN のマルチキャスト グループ数を表示します。   |
|       | <b>dynamic</b>                | (任意) MLD スヌーピング学習グループ情報を表示します。  |
|       | <b>user</b>                   | (任意) MLD スヌーピング ユーザ設定グループ情報を表示します。  |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン**

IPv6 マルチキャスト アドレス情報を表示するのに、このコマンドを使用します。VLAN ID を入力した後に限り、IPv6 マルチキャスト アドレスを入力できます。1002 ~ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

学習されたグループに関する情報だけを表示するには、**dynamic** キーワードを使用します。設定されたグループに関する情報だけを表示するには、**user** キーワードを使用します。

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



**(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。

## ■ show ipv6 mld snooping address

## 例

次の例では、**show ipv6 mld snooping address EXEC** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address
Vlan Group   Type Version Port List
-----
2    FF12::3 user           Fa1/2, Gi1/2, Gi1/1,Gi1/3
```

次の例では、**show ipv6 mld snooping address count EXEC** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address count
Total number of multicast groups: 2
```

次の例では、**show ipv6 mld snooping address ユーザ** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address user
Vlan Group   Type Version Port List
-----
2    FF12::3 user   v2    Fa1/2, Gi1/2, Gi1/1,Gi1/3
```

## 関連コマンド

| コマンド                                   | 説明   |
|--|--|
| <a href="#">ipv6 mld snooping vlan</a> | VLAN で IPv6 MLD スヌーピングを設定します。                    |
| <a href="#">sdm prefer</a>             | スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。 |

# show ipv6 mld snooping mrouter

スイッチまたは VLAN に対してダイナミックに学習され、手動で設定された IP version 6 (IPv6) マルチキャストリスナー検出 (MLD) ルータ ポートを表示するには、**show ipv6 mld snooping mrouter** コマンドを使用します。

```
show ipv6 mld snooping mrouter [vlan vlan-id]
```

|       |   |
|-------|---|
| 構文の説明 | <b>vlan <i>vlan-id</i></b> (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。 |
|-------|---|

|       |    |
|-------|----|
| デフォルト | なし |
|-------|----|

|         |      |
|---------|------|
| コマンドモード | EXEC |
|---------|------|

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**使用上のガイドライン** スイッチまたは特定の VLAN の MLD スヌーピング ルータ ポートを表示するには、このコマンドを使用します。

1002 ~ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

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



**(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。

**例** 次の例では、**show ipv6 mld snooping mrouter** コマンドの出力を示します。MLD スヌーピングに参加する、スイッチのすべての VLAN のスヌーピング特性が表示されます。

```
Switch> show ipv6 mld snooping mrouter
Vlan      ports
----      -
    2      Gi1/11 (dynamic)
   72      Gi1/11 (dynamic)
  200      Gi1/11 (dynamic)
```

次の例では、**show ipv6 mld snooping mrouter vlan** コマンドの出力を示します。特定の VLAN のマルチキャスト ルータ ポートが表示されます。

```
Switch> show ipv6 mld snooping mrouter vlan 100
Vlan      ports
----      -
    2      Gi1/11 (dynamic)
```

## ■ show ipv6 mld snooping mrouter

| 関連コマンド | コマンド   | 説明  |
|--------|--|---|
|        | <b>ipv6 mld snooping</b>   | スイッチ上または VLAN 上の MLD スヌーピングをイネーブルにし、設定を行います。      |
|        | <b>ipv6 mld snooping vlan mrouter interface interface-id   static ipv6-multicast-address interface interface-id]</b> | VLAN にマルチキャスト ルータ ポートを設定します。                      |
|        | <b>sdm prefer</b>  | 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に SDM テンプレートを設定します。 |

# show ipv6 mld snooping querier

スイッチまたは VLAN によって直近に受信した IP version 6 (IPv6) マルチキャストリスナー検出 (MLD) スヌーピング クエリア関連情報を表示するには、EXEC モードで **show ipv6 mld snooping querier** コマンドを使用します。

**show ipv6 mld snooping querier [vlan *vlan-id*] [detail]**



(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   | <b>vlan <i>vlan-id</i></b> (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。 |
|         | <b>detail</b> (任意) スイッチまたは VLAN の MLD スヌーピングの詳細なクエリア情報を表示します。                     |
| デフォルト   | なし  |
| コマンドモード | EXEC  |
| コマンド履歴  | リリース<br>15.0(1)EY   |
|         | 変更内容<br>このコマンドが導入されました。   |

## 使用上のガイドライン

MLD クエリー メッセージを送信する検出された装置 (クエリアとも呼ばれる) の MLD バージョンおよび IPv6 アドレスを表示するには、**show ipv6 mld snooping querier** コマンドを使用します。サブネットワークは複数のマルチキャスト ルータを持つことができますが、MLD クエリアは 1 つだけです。クエリアには、レイヤ 3 スイッチを指定できます。

**show ipv6 mld snooping querier** コマンド出力は、クエリアが検出された VLAN およびインターフェイスも表示します。クエリアがスイッチの場合、出力では **Port** フィールドに **Router** が表示されます。クエリアがルータの場合、出力では、**Port** フィールドにクエリアを学習したポート番号が表示されません。

**show ipv6 mld snooping querier vlan** コマンドの出力では、外部または内部クエリアからのクエリー メッセージに回答して受信された情報を表示します。特定の VLAN 上のスヌーピング ロバストネス変数などのユーザ設定の VLAN 値は表示されません。このクエリア情報は、スイッチが送信する MASQ メッセージ上だけで使用されます。クエリー メッセージに回答しないメンバを期限切れにするのに使用するユーザ設定のロバストネス変数は無効にはなりません。

1002 ~ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

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

文字列では、大文字と小文字が区別されます。たとえば、**exclude output** と入力した場合、**output** を含む行は表示されませんが、**Output** を含む行は表示されます。

## ■ show ipv6 mld snooping querier

## 例

次の例では、**show ipv6 mld snooping querier** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier
Vlan      IP Address          MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1      Gi1/1
```

次の例では、**show ipv6 mld snooping querier detail** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier detail
Vlan      IP Address          MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1      Gi1/1
```

次の例では、**show ipv6 mld snooping querier vlan** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier vlan 2
IP address : FE80::201:C9FF:FE40:6000
MLD version : v1
Port : Gi1/1
Max response time : 1000s
```

## 関連コマンド

| コマンド   | 説明   |
|--|--|
| <a href="#">ipv6 mld snooping</a>                              | スイッチ上または VLAN 上の IPv6 MLD スヌーピングをイネーブルにし、設定を行います。          |
| <a href="#">ipv6 mld snooping last-listener-query-count</a>    | MLD クライアントが期限切れになる前にスイッチが送信するクエリーの最大数を設定します。               |
| <a href="#">ipv6 mld snooping</a>                              | スイッチ上または VLAN 上の IPv6 MLD スヌーピングをイネーブルにし、設定を行います。          |
| <a href="#">ipv6 mld snooping last-listener-query-interval</a> | スイッチがクエリーを送信してから、マルチキャスト グループからポートを削除する前に待機する最大応答時間を設定します。 |
| <a href="#">ipv6 mld snooping robustness-variable</a>          | 応答がない場合、マルチキャスト アドレスが期限切れになる前にスイッチが送信するクエリーの最大数を設定します。     |
| <a href="#">sdm prefer</a>                                     | 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に SDM テンプレートを設定します。          |

# 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、EXEC コマンドの **show ipv6 route updated** コマンドを使用します。

```
show ipv6 route updated [boot-up]{hh:mm | day{month [hh:mm]} [{hh:mm | day{month [hh:mm]}}
```

## 構文の説明

|                |   |
|----------------|---|
| <b>boot-up</b> | (任意) 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 桁の数値で入力されている時刻。必ずコロン (:) を使用してください。たとえば、 <b>13:32</b> のように入力します。   |
| <i>day</i>     | 日付。指定できる範囲は 1 ~ 31 です。  |
| <i>month</i>   | 大文字または小文字で入力されている月。 <b>January</b> または <b>august</b> など、月の名前をすべて入力することも、 <b>jan</b> または <b>Aug</b> 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。 |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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:CFFF:FE00:8D01, GigabitEthernet1/1
Last updated 10:31:10 27 February 2007
R 2004::/64 [120/2]
via FE80::A8BB:CFFF:FE00:9001, GigabitEthernet1/2
Last updated 17:23:05 22 February 2007
R 4000::/64 [120/2]
via FE80::A8BB:CFFF:FE00:9001, GigabitEthernet1/3
Last updated 17:23:05 22 February 2007
R 5000::/64 [120/2]
via FE80::A8BB:CFFF:FE00:9001, GigabitEthernet1/4
```

## ■ show ipv6 route updated

```
Last updated 17:23:05 22 February 2007
R 5001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/5
Last updated 17:23:05 22 February 2007
```

## 関連コマンド

| コマンド            | 説明  |
|-----------------|---|
| show ipv6 route | IPv6 ルーティング テーブルの現在の内容を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# show l2nat instance

レイヤ 2 NAT インスタンスの構成の詳細を表示するには、EXEC モードで、**show l2nat instance** コマンドを入力します。

```
show l2nat instance [instance_name]
```

|       |                      |   |
|-------|----------------------|---|
| 構文の説明 | <i>instance_name</i> | (任意) 表示するレイヤ 2 NAT インスタンス。このパラメータを省略すると、すべてのレイヤ 2 NAT のインスタンスが表示されます。 |
|-------|----------------------|---|

コマンドデフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(2)EB | このコマンドが導入されました。 |

例 次に、すべてのレイヤ 2 NAT インスタンス設定の詳細を表示する例を示します。

```
Switch# show l2nat instance
l2nat instance Instance3
  fixup : arp, icmp
  inside from host 10.10.20.5 to 10.10.30.5
l2nat instance Instance2
  fixup : arp, icmp
  inside from host 10.10.11.1 to 10.10.12.1
l2nat instance Instance1
  fixup : arp, icmp
  inside from host 10.10.10.1 to 20.20.20.1
```

| 関連コマンド | コマンド  | 説明  |
|--------|---|---|
|        | <a href="#">inside from</a>                     | レイヤ 2 NAT を使用して内部アドレスを外部アドレスに変換します。                         |
|        | <a href="#">l2nat</a>                           | 選択したインターフェイスの 1 つまたはすべての VLAN にレイヤ 2 NAT インスタンスを適用します。      |
|        | <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
|        | <a href="#">outside from</a>                    | レイヤ 2 NAT を使用して、外部アドレスを内部アドレスに変換します。                        |
|        | <a href="#">show l2nat interface</a>            | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。                |
|        | <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |
|        | <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# show l2nat interface

特定のインターフェイスや VLAN のレイヤ 2 NAT インスタンスの構成の詳細を表示するには、EXEC モードで、**show l2nat interface** コマンドを使用します。インターフェイスまたは VLAN を指定しない場合、すべてが含まれます。

**show l2nat interface** [*int*] [*vlan*]

| 構文の説明       |  |
|-------------|--|
| <i>int</i>  | (任意) インターフェイス。このパラメータを省略した場合は、すべてのインターフェイスが含まれます。                                  |
| <i>vlan</i> | (任意) VLAN ID インターフェイスが指定されている場合にだけ、このパラメータが含まれます。このパラメータを省略した場合は、すべての VLAN が含まれます。 |

コマンド デフォルト なし

コマンド モード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(2)EB | このコマンドが導入されました。 |

例 次に、すべてのインターフェイスのすべてのレイヤ 2 NAT インスタンスの設定の詳細を表示する例を示します。

```
Switch# show l2nat interface
FOLLOWING INSTANCES ARE ATTACHED TO INTERFACE Gi1/2
=====

INSTANCE ATTACHED TO VLAN 24
l2nat instance Instance1
  fixup : arp, icmp
  inside from host 10.10.11.1 to 10.10.12.1
=====
FOLLOWING INSTANCES ARE ATTACHED TO INTERFACE Gi1/1
=====

INSTANCE ATTACHED TO VLAN 11
l2nat instance Instance2
  fixup : arp, icmp
  inside from host 10.10.11.1 to 10.10.12.1
=====
FOLLOWING INSTANCES ARE ATTACHED TO INTERFACE Gi1/1
=====

INSTANCE ATTACHED TO VLAN 6
l2nat instance Instance3
  fixup : arp, icmp
  inside from host 10.10.20.6 to 10.10.30.6
```

次の例では、インターフェイス Gi1/1、VLAN 10 のレイヤ 2 NAT インスタンス設定の詳細を表示する例を示します。

```
Switch# show l2nat interface Gi1/1 10
FOLLOWING INSTANCES ARE ATTACHED TO INTERFACE Gi1/1
=====

INSTANCE ATTACHED TO VLAN 10
l2nat instance Instance2
  fixup : arp, icmp
  inside from host 10.10.11.1 to 10.10.12.1
=====
FOLLOWING INSTANCES ARE ATTACHED TO INTERFACE Gi1/1
=====
```

### 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                           |
| <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# show l2nat statistics

すべてのレイヤ 2 NAT インスタンスの統計情報を表示するには、EXEC モードで **show l2nat statistics** コマンドを使用します。

## show l2nat 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。

### コマンドデフォルト

なし

### コマンドモード

EXEC

### 使用上のガイドライン

各レイヤ 2 NAT のインスタンスでは、統計情報には、バイパスされた、破棄された、変換されたパケット数の他、ARP、ICMP、NSMP、PROFINET のフィックスアップ数や、IGMP、マルチキャスト、一致しない、ユニキャストのパケット数が含まれます。これらすべてについてのグローバル統計情報もあります。

追加の統計情報には、過去 90 秒間のアクティブな変換数、合計変換数、およびインターフェイスに接続された合計インスタンスの数が含まれます。

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(2)EB | このコマンドが導入されました。 |

### 例

次に、すべての l2nat 統計情報を表示する例を示します。

```
Switch# show l2nat statistics

STATS FOR INSTANCE: NewInstance1 (IN PACKETS)

TRANSLATED STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  BYPASSED   DISCARDED   TRANSLATED   TOTAL PACKETS
Gi1/1     EGRESS      10         0           153         127305106    127305259
Gi1/1     INGRESS    10         0           0           127305104    127305105
-----

PROTOCOL FIXUP STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  ARP        ICMP        SNMP        PROFINET
Gi1/1     EGRESS      10      1           0           0           0
Gi1/1     INGRESS    10      1           0           0           0
-----

IGMP AND MULTICAST STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  IGMP        MULTICAST   UNMATCHED   UNICAST
Gi1/1     EGRESS      10      0           1134        1150        127304124
Gi1/1     INGRESS    10      0           0           0           127305103
-----
```

```

PER TRANSLATION STATS (IN PACKETS)
=====
TYPE      DIRECTION SA/DA ORIGINAL IP    TRANSLATED IP    COUNT    ACTIVE (90Sec)
INSIDE    EGRESS    SA    172.16.1.1     20.1.1.1         127305166 4847525
INSIDE    INGRESS   DA    20.1.1.1       172.16.1.1       127305165 4847525
OUTSIDE   INGRESS   SA    20.1.1.254     172.16.1.254     1          0
OUTSIDE   EGRESS    DA    172.16.1.254   20.1.1.254       1          0
=====

```

STATS FOR INSTANCE: NewInstance2 (IN PACKETS)

```

TRANSLATED STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  BYPASSED  DISCARDED  TRANSLATED  TOTAL PACKETS
Gi1/1     EGRESS   4094  9588      0           127305222   127314836
Gi1/1     INGRESS  4094   0         0           127305222   127305222
=====

```

```

PROTOCOL FIXUP STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  ARP      ICMP      SNMP      PROFINET
Gi1/1     EGRESS   4094  1         0         0         0
Gi1/1     INGRESS  4094  1         0         0         0
=====

```

```

IGMP AND MULTICAST STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  IGMP      MULTICAST  UNMATCHED  UNICAST
Gi1/1     EGRESS   4094  0         8464       8624       127306355
Gi1/1     INGRESS  4094  0         0          0          127305222
=====

```

```

PER TRANSLATION STATS (IN PACKETS)
=====
TYPE      DIRECTION SA/DA ORIGINAL IP    TRANSLATED IP    COUNT    ACTIVE (90Sec)
OUTSIDE   INGRESS   SA    10.1.1.254     192.168.1.254   1          0
OUTSIDE   EGRESS    DA    192.168.1.254  10.1.1.254      1          0
INSIDE    EGRESS    SA    192.168.1.1    10.1.1.1         127305292 4847645
INSIDE    INGRESS   DA    10.1.1.1       192.168.1.1     127305292 4847645
=====

```

```

NUMBER OF ACTIVE TRANSLATIONS IN THE PAST 90 SECONDS: 2
TOTAL TRANSLATIONS : 4
TOTAL INSTANCES ATTACHED: 2
=====

```

```

GLOBAL NAT STATISTICS
=====
Total Number of NAT Packets           = 509230422
Total Number of TRANSLATED NAT Packets = 509220654
Total Number of BYPASSED NAT Packets   = 9588
Total Number of DISCARDED NAT Packets  = 153
Total Number of ARP FIX UP Packets     = 4
Total Number of ICMP FIX UP Packets    = 0
Total Number of SNMP FIX UP Packets    = 0
Total Number of PROFINET FIX UP Packets = 0
Total Number of IPV4 MULTICAST Packets = 9598
Total Number of IGMP Packets           = 0
Total Number of UNMATCHED Packets     = 9774
Total Number of IPV4 UNICAST Packets   = 509220804
=====

```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                           |
| <a href="#">show l2nat interface</a>            | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。                |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# show l2nat statistics interface

指定したインターフェイスまたは VLAN の統計情報を表示するには、EXEC モードで **show l2nat statistics interface** コマンドを使用します。

**show l2nat statistics interface** [*int*] [*vlan*]

| 構文の説明 | パラメータ       | 説明  |
|-------|-------------|---|
|       | <i>int</i>  | インターフェイス。このパラメータを省略した場合は、すべてのインターフェイスが含まれます。                                  |
|       | <i>vlan</i> | VLAN ID。インターフェイスが指定されている場合にだけ、このパラメータが含まれます。このパラメータを省略した場合は、すべての VLAN が含まれます。 |

コマンドデフォルト なし

コマンドモード EXEC

**使用上のガイドライン** インターフェイスまたは VLAN を指定しない場合、すべてが含まれます。統計情報には、バイパスされた、破棄された、変換されたパケット数の他、ARP、ICMP、パススルー プロトコル SNMP、PROFINET、SIP、PTP、Telnet、FTP のフィックスアップ数や、IGMP、マルチキャスト、一致しない、ユニキャストのパケット数が含まれます。

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(2)EB | このコマンドが導入されました。 |

**例** この例では、インターフェイス Gi1/1、VLAN10 の l2nat 統計情報を表示する例を示します。

```
Switch# show l2nat statistics interface Gi1/1 10

TRANSLATED STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  BYPASSED   DISCARDED   TRANSLATED   TOTAL PACKETS
Gi1/1      EGRESS      10         0           153          127305106    127305259
Gi1/1      INGRESS     10         0           0            127305104    127305105
=====

PROTOCOL FIXUP STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  ARP      ICMP      SNMP      PROFINET
Gi1/1      EGRESS     10      1         0         0         0
Gi1/1      INGRESS    10      1         0         0         0
=====

IGMP AND MULTICAST STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  IGMP      MULTICAST  UNMATCHED  UNICAST
Gi1/1      EGRESS     10      0         1134       1150       127304124
Gi1/1      INGRESS    10      0         0          0          127305103
=====
```

## ■ show l2nat statistics interface

## 関連コマンド

| コマンド                                  | 説明  |
|---------------------------------------|---|
| <a href="#">l2nat instance</a>        | レイヤ 2 NAT インスタンスを作成するか、または指定したレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">show l2nat instance</a>   | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                           |
| <a href="#">show l2nat interface</a>  | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。                |
| <a href="#">show l2nat statistics</a> | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                          |

# 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、EXEC モードで **show lacp** コマンドを使用します。

```
show lacp [channel-group-number] {counters | internal | neighbor | sys-id}
```

## 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 ~ 6 です。   |
| <b>counters</b>             | トラフィック情報を表示します。   |
| <b>internal</b>             | 内部情報を表示します。   |
| <b>neighbor</b>             | ネイバーの情報を表示します。  |
| <b>sys-id</b>               | LACP によって使用されるシステム識別子を表示します。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。 |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 例

次の例では、**show lacp counters** EXEC コマンドの出力を示します。表 2-28 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
Gi1/1      19   10         0     0         0     0         0
Gi1/2      14    6         0     0         0     0         0
```

表 2-28 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 |

表 2-28 show lacp counters のフィールドの説明 (続き)

| フィールド                         | 説明                                |
|-------------------------------|-----------------------------------|
| Marker Response Sent および Recv | ポートによって送受信された LACP Marker 応答パケット数 |
| LACPDUs Pkts および Err          | ポートの LACP によって受信された、未知で不正なパケット数   |

これは、**show lacp channel-group-number internal** のコマンド出力例を示します。

```
Switch> show lacp 1 internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1

Port      Flags  State  LACP port  Admin  Oper  Port  Port
          State Priority Key      Key      Number State
Gi1/1    SA     bndl   32768      0x3    0x3    0x4   0x3D
Gi1/2    SA     bndl   32768      0x3    0x3    0x5   0x3D
```

表 2-29 に、この出力で表示されるフィールドの説明を示します。

表 2-29 show lacp internal のフィールドの説明

| フィールド              | 説明   |
|--------------------|--|
| State              | 特定のポートの状態。次に使用可能な値を示します。 <ul style="list-style-type: none"> <li>– : ポートは <b>unknown</b> ステートです。</li> <li><b>bndl</b> : 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。</li> <li><b>susp</b> : 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。</li> <li><b>hot-sby</b> : ポートがホットスタンバイの状態です。</li> <li><b>indiv</b> : ポートを他のポートとともにバンドルできません。</li> <li><b>indep</b> : ポートは <b>independent</b> 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。</li> <li><b>down</b> : ポートがダウンしています。</li> </ul> |
| LACP Port Priority | ポートのプライオリティ設定。互換性のあるすべてのポートが集約することを妨げる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を使ってポートをスタンバイモードにします。   |
| Admin Key          | ポートに割り当てられた管理用のキー。LACP は自動的に管理用のキー値を生成します (16 進数)。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。その他のポートと集約されるポートの機能は、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、設定時の制約事項によって決まります。   |
| 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す (16 進数)。   |

表 2-29 show lacp internal のフィールドの説明 (続き)

| フィールド       | 説明   |
|-------------|--|
| 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"> <li>• bit0 : LACP のアクティビティ</li> <li>• bit1 : LACP のタイムアウト</li> <li>• bit2 : 集約</li> <li>• bit3 : 同期</li> <li>• bit4 : 収集</li> <li>• bit5 : 配信</li> <li>• bit6 : デフォルト</li> <li>• bit7 : 期限切れ</li> </ul> <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 | Partner Age | Partner Flags |
|-------|----------------------|---------------------|-------------|---------------|
| Gi1/1 | 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 | Partner Age | Partner Flags |
|-------|----------------------|---------------------|-------------|---------------|
| Gi1/2 | 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。

## ■ show lacp

## 関連コマンド

| コマンド                                 | 説明                       |
|--------------------------------------|--------------------------|
| <a href="#">clear lacp</a>           | LACP チャンネル グループ情報を消去します。 |
| <a href="#">lacp port-priority</a>   | LACP ポート プライオリティを設定します。  |
| <a href="#">lacp system-priority</a> | LACP システム プライオリティを設定します。 |

# show link-diag error-rate

リンクの診断エラー レートの情報を表示するには、特権 EXEC モードで **show link state group** コマンドを使用します。

```
show link-diag error-rate {fastethernet interface | gigabitethernet interface | window-size}
```

| 構文の説明 | パラメータ                            | 説明   |
|-------|----------------------------------|--|
|       | <b>fastethernet interface</b>    | 1-1 からの範囲で fastethernet インターフェイス番号を表示します。    |
|       | <b>gigabitethernet interface</b> | 1-1 からの範囲で gigabitethernet インターフェイス番号を表示します。 |
|       | <b>window-size</b>               | リンクの診断エラー レートのウィンドウ サイズを表示します。               |

**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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**例** 次に、リンクの診断エラー レートを表示する例を示します。

```
Switch# show link-diag error-rate
Port      Receive Err-Rate  Transmit Err-Rate
----      -
Fa1/1     0                  0
Fa1/2     0                  0
Fa1/3     0                  0
Fa1/4     0                  0
Gi1/1     0                  0
Gi1/2     0                  0
Switch#
```

次に、ファストイーサネットリンクで診断エラー レートを表示する例を示します。

```
Switch# show link-diag error-rate fastethernet 1/1
Port      Receive Err-Rate  Transmit Err-Rate
----      -
Fa1/1     0                  0
Switch#
```

次に、ギガビットイーサネットリンクの診断エラー レートを表示する例を示します。

```
Switch# show link-diag error-rate gigabitethernet 1/1
Port      Receive Err-Rate  Transmit Err-Rate
----      -
Gi1/1     0                  0
Switch#
```

| 関連コマンド | コマンド                                 | 説明                        |
|--------|--------------------------------------|---------------------------|
|        | <a href="#">link-diag error-rate</a> | リンクの診断機能のウィンドウ サイズを設定します。 |

# show location

エンドポイントのロケーション情報を表示するには、EXEC モードで **show location** コマンドを使用します。

```
show location [admin-tag] [civic-location | elin-location {cdp | identifier id | interface
interface-id | static}]
```

## 構文の説明

|                               |  |
|-------------------------------|--|
| <b>admin-tag</b>              | (任意) 管理タグまたはサイト情報を表示します。   |
| <b>civic-location</b>         | (任意) 都市ロケーション情報を表示します。   |
| <b>elin-location</b>          | (任意) 緊急ロケーション情報 (ELIN) を表示します。   |
| <b>cdp</b>                    | (任意) CDP ロケーション情報を表示します。   |
| <b>identifier id</b>          | (任意) 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。              |
| <b>interface interface-id</b> | (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。 |
| <b>static</b>                 | (任意) ホスタティック コンフィギュレーション情報を表示します。  |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## 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 gigibitethernet1/1
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 identifier** 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              : Gi1/1
-----
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    : Gi1/2
```

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    : Gi1/2
-----
Identifier : 2
Elin      : 18002228999
-----
```

## 関連コマンド

| コマンド                                   | 説明                            |
|--|-------------------------------|
| <b>location</b> (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。 |
| <b>location</b> (インターフェイス コンフィギュレーション) | インターフェイスにロケーション情報を設定します。      |

# show link state group

リンク ステート グループ情報を表示するには、特権 EXEC モードで **show link state group** コマンドを使用します。

**show link state group** [*number*] [*detail*]

|       |               |                         |
|-------|---------------|-------------------------|
| 構文の説明 | <i>number</i> | (任意) リンクステート グループの番号です。 |
|       | <i>detail</i> | (任意) 詳細情報を表示するように指定します。 |

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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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。

**例**

次の例では、**show link state group 1** コマンドの出力を示します。

```
Switch> show link state group 1
Link State Group: 1      Status: Enabled, Down
```

次の例では、**show link state group detail** コマンドの出力を示します。

```
Switch> show link state group detail
(Up):Interface up      (Dwn):Interface Down  (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi1/1(Dwn) Gi1/2(Dwn)
Downstream Interfaces : Fa1/5(Dis) Fa1/6(Dis) Fa1/7(Dis) Fa1/8(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi1/1(Dwn) Gi1/2(Dwn) Gi1/3(Dwn)
Downstream Interfaces : Fa1/5(Dis) Fa1/6(Dis) Fa1/7(Dis) Fa1/8(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

## 関連コマンド

| コマンド                             | 説明                                 |
|----------------------------------|------------------------------------|
| <a href="#">link state group</a> | 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。 |
| <a href="#">link state track</a> | リンクステート グループをイネーブルにします。            |

# show mac access-group

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、EXEC モードで **show mac access-group** コマンドを使用します。

**show mac access-group interface *interface-id***

|       |  |
|-------|--|
| 構文の説明 | <b>interface <i>interface-id</i></b> (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 1～6 です (特権 EXEC モードでのみ使用可能)。 |
|-------|--|

|       |    |
|-------|----|
| デフォルト | なし |
|-------|----|

|         |      |
|---------|------|
| コマンドモード | EXEC |
|---------|------|

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**例** 次の例では、**show mac-access group EXEC** コマンドの出力を示します。ポート 2 には、適用される MAC アクセス リスト `macl_e1` があります。MAC ACL は他のインターフェイスに適用されません。

```
Switch> show mac access-group
Interface GigabitEthernet1/1:
  Inbound access-list is not set
Interface GigabitEthernet1/2:
  Inbound access-list is macl_e1
Interface GigabitEthernet1/3:
  Inbound access-list is not set
Interface GigabitEthernet1/4:
  Inbound access-list is not set
```

<output truncated>

次の例では、**show mac access-group interface** コマンドの出力を示します。

```
Switch# show mac access-group interface gigabitethernet1/1
Interface GigabitEthernet1/1:
  Inbound access-list is macl_e1
```

| 関連コマンド | コマンド                             | 説明                             |
|--------|----------------------------------|--------------------------------|
|        | <a href="#">mac access-group</a> | 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

特定のインターフェイスまたは VLAN の特定の 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 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、EXEC モードで **show mac address-table** コマンドを使用します。

## show mac address-table

### 構文の説明

このコマンドにはキーワードまたは引数はありません。

### デフォルト

なし

### コマンド モード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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   Gi1/2
Total Mac Addresses for this criterion: 12
```

## 関連コマンド

| コマンド                                       | 説明   |
|--|--|
| <b>clear mac address-table dynamic</b>     | 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。 |
| <b>show mac address-table aging-time</b>   | 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。  |
| <b>show mac address-table count</b>        | 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。  |
| <b>show mac address-table dynamic</b>      | 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。   |
| <b>show mac address-table interface</b>    | 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。  |
| <b>show mac address-table notification</b> | 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。   |
| <b>show mac address-table static</b>       | 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。   |
| <b>show mac address-table vlan</b>         | 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

特定の MAC アドレスの MAC アドレス テーブル情報を表示するには、EXEC モードで **show mac address-table address** コマンドを使用します。

```
show mac address-table address mac-address [interface interface-id] [vlan vlan-id]
```

| 構文の説明 | パラメータ                                | 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。                       |
|       | <b>interface</b> <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 チャネルが含まれます。 |
|       | <b>vlan</b> <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。             |

デフォルト なし

コマンド モード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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   |
|---|--|
| <a href="#">show mac address-table aging-time</a>   | 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。            |
| <a href="#">show mac address-table count</a>        | 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。          |
| <a href="#">show mac address-table dynamic</a>      | 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。                   |
| <a href="#">show mac address-table interface</a>    | 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。                |
| <a href="#">show mac address-table notification</a> | 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。 |
| <a href="#">show mac address-table static</a>       | 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。                   |
| <a href="#">show mac address-table vlan</a>         | 指定された VLAN の MAC アドレス テーブル情報を表示します。                  |

# show mac address-table aging-time

特定のアドレス テーブル インスタンスのエージング タイム、指定された VLAN 上または指定がない場合はすべての VLAN 上のすべてのアドレス テーブル インスタンスのエージング タイムを表示するには、**show mac address-table aging-time** コマンドを EXEC モードで使用します。

```
show mac address-table aging-time [vlan vlan-id]
```

|          |                            |  |
|----------|----------------------------|--|
| 構文の説明    | <b>vlan <i>vlan-id</i></b> | (任意) 特定の VLAN のエージング タイム情報を表示します。指定できる範囲は 1 ~ 4094 です。 |
| デフォルト    | なし                         |  |
| コマンド モード | EXEC                       |  |
| コマンド履歴   | リリース                       | 変更内容   |
|          | 15.0(1)EY                  | このコマンドが導入されました。  |

## 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 に対するエージング タイムが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show mac address-table aging-time** コマンドの出力を示します。

```
Switch> show mac address-table aging-time
Vlan      Aging Time
-----
1         300
```

次の例では、**show mac address-table aging-time vlan 10** コマンドの出力を示します。

```
Switch> show mac address-table aging-time vlan 10
Vlan      Aging Time
-----
10        300
```

## ■ show mac address-table aging-time

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">mac address-table aging-time</a>        | 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。 |
| <a href="#">show mac address-table address</a>      | 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。                |
| <a href="#">show mac address-table count</a>        | 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。           |
| <a href="#">show mac address-table dynamic</a>      | 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。                    |
| <a href="#">show mac address-table interface</a>    | 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。                 |
| <a href="#">show mac address-table notification</a> | 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。  |
| <a href="#">show mac address-table static</a>       | 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。                    |
| <a href="#">show mac address-table vlan</a>         | 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、EXEC モードで **show mac address-table count** コマンドを使用します。

```
show mac address-table count [vlan vlan-id]
```

|       |   |
|-------|---|
| 構文の説明 | <b>vlan <i>vlan-id</i></b> (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。 |
|-------|---|

|       |    |
|-------|----|
| デフォルト | なし |
|-------|----|

|         |      |
|---------|------|
| コマンドモード | EXEC |
|---------|------|

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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
```

## ■ show mac address-table count

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">show mac address-table address</a>      | 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。               |
| <a href="#">show mac address-table aging-time</a>   | 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。            |
| <a href="#">show mac address-table dynamic</a>      | 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。                   |
| <a href="#">show mac address-table interface</a>    | 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。                |
| <a href="#">show mac address-table notification</a> | 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。 |
| <a href="#">show mac address-table static</a>       | 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。                   |
| <a href="#">show mac address-table vlan</a>         | 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、EXEC モードで **show mac address-table dynamic** コマンドを使用します。

**show mac address-table dynamic** [*address mac-address*] [*interface interface-id*] [*vlan vlan-id*]

## 構文の説明

|                               |   |
|-------------------------------|---|
| <b>address mac-address</b>    | (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)。 |
| <b>interface interface-id</b> | (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。            |
| <b>vlan vlan-id</b>           | (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。                         |

## デフォルト

なし

## コマンド モード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 Gi1/2
1       00b0.6496.2741   DYNAMIC Gi1/2
Total Mac Addresses for this criterion: 2
```

## ■ show mac address-table dynamic

## 関連コマンド

| コマンド                                     | 説明   |
|--|--|
| <b>clear mac address-table dynamic</b>   | 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。 |
| <b>show mac address-table address</b>    | 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。   |
| <b>show mac address-table aging-time</b> | 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。  |
| <b>show mac address-table count</b>      | 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。  |
| <b>show mac address-table interface</b>  | 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。  |
| <b>show mac address-table static</b>     | 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。   |
| <b>show mac address-table vlan</b>       | 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

指定した VLAN の指定し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 user** コマンドを使用します。

```
show mac address-table interface interface-id [vlan vlan-id]
```

| 構文の説明 | interface-id | (任意) インターフェイス タイプを指定します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。 |
|-------|--------------|---|
|       | vlan vlan-id | (任意) 特定の VLAN のエントリを表示します。指定できる範囲は 1 ~ 4094 です。             |

デフォルト なし

コマンド モード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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 gigabitethernet1/2
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
  1     0030.b635.7862  DYNAMIC Gi1/2
  1     00b0.6496.2741  DYNAMIC Gi1/2
Total Mac Addresses for this criterion: 2
```

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">show mac address-table address</a>      | 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。               |
| <a href="#">show mac address-table aging-time</a>   | 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。            |
| <a href="#">show mac address-table count</a>        | 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。          |
| <a href="#">show mac address-table dynamic</a>      | 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。                   |
| <a href="#">show mac address-table notification</a> | 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。 |
| <a href="#">show mac address-table static</a>       | 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。                   |
| <a href="#">show mac address-table vlan</a>         | 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 ステータスを表示するには、EXEC モードで **show mac address-table learning** コマンドを使用します。

**show mac address-table learning [vlan *vlan-id*]**

|       |  |
|-------|--|
| 構文の説明 | <b>vlan <i>vlan-id</i></b> (任意) 特定の VLAN の情報を表示します。指定できる範囲は 1 ~ 4094 です。 |
|-------|--|

|       |    |
|-------|----|
| デフォルト | なし |
|-------|----|

|         |      |
|---------|------|
| コマンドモード | EXEC |
|---------|------|

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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 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  |
|--------|---|---|
|        | <a href="#">mac address-table learning vlan</a> | 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

MAC アドレス テーブル移動更新情報を表示するには、スイッチの更新情報を、EXEC モードで **show mac address-table move update** コマンドを使用します。

## show mac address-table move update

### 構文の説明

このコマンドにはキーワードまたは引数はありません。

### デフォルト

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、**output** を含む行は表示されませんが、*Output* を含む行は表示されます。

### 例

次の例では、**show mac address-table move update** コマンドの出力を示します。

```
Switch> show mac address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
switch#
```

### 関連コマンド

| コマンド   | 説明                              |
|--|---------------------------------|
| <a href="#">clear mac address-table move update</a>                | MAC アドレス テーブル移行更新カウンタをクリアします。   |
| <a href="#">mac address-table move update {receive   transmit}</a> | 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、EXEC モードで **show mac address-table notification** コマンドを使用します。

```
show mac address-table notification {change [interface [interface-id] | mac-move | threshold]}
```

## 構文の説明

|                     |  |
|---------------------|--|
| <b>change</b>       | 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。                                |
| <b>interface</b>    | (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。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。         |
| <b>mac-move</b>     | MAC アドレス移動通知の表示状態。   |
| <b>threshold</b>    | MAC アドレス テーブルのしきい値モニタリングの状態を表示します。                             |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

## ■ show mac address-table notification

## 例

次の例では、**show mac address-table notification change** コマンドの出力を示します。

```
Switch> show mac address-table notification change
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
-----
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added   Vlan: 2       MAC Addr: 0000.0000.0001 Module: 0   Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added   Vlan: 2       MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Added   Vlan: 2       MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Added   Vlan: 2       MAC Addr: 0000.0000.0003 Module: 0   Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2       MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Deleted Vlan: 2       MAC Addr: 0000.0000.0001 Module: 0   Port: 1
Operation: Deleted Vlan: 2       MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Deleted Vlan: 2       MAC Addr: 0000.0000.0003 Module: 0   Port: 1
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <b>clear mac address-table notification</b> | MAC アドレス通知グローバル カウンタをクリアします。                            |
| <b>mac address-table notification</b>       | MAC アドレス変更、移動、またはアドレス テーブルしきい値の MAC アドレス通知機能をイネーブルにします。 |
| <b>show mac address-table address</b>       | 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。                  |
| <b>show mac address-table aging-time</b>    | 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。               |
| <b>show mac address-table count</b>         | 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。             |
| <b>show mac address-table dynamic</b>       | 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。                      |
| <b>show mac address-table interface</b>     | 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。                   |
| <b>show mac address-table static</b>        | 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。                      |
| <b>show mac address-table vlan</b>          | 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、EXEC モードで **show mac address-table static** コマンドを使用します。

**show mac address-table static** [*address mac-address*] [*interface interface-id*] [*vlan vlan-id*]

| 構文の説明 | パラメータ                                | 説明  |
|-------|--------------------------------------|---|
|       | <b>address</b> <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)。 |
|       | <b>interface</b> <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 チャネルが含まれます。            |
|       | <b>vlan</b> <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。                         |

デフォルト なし

コマンド モード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

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
```

## ■ show mac address-table static

## 関連コマンド

| コマンド                                       | 説明   |
|--|--|
| <b>mac address-table static</b>            | 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。   |
| <b>mac address-table static drop</b>       | 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。 |
| <b>show mac address-table address</b>      | 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。   |
| <b>show mac address-table aging-time</b>   | 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。  |
| <b>show mac address-table count</b>        | 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。  |
| <b>show mac address-table dynamic</b>      | 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。   |
| <b>show mac address-table interface</b>    | 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。  |
| <b>show mac address-table notification</b> | 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。                               |
| <b>show mac address-table vlan</b>         | 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

特定の VLAN の MAC アドレス テーブル情報を表示するには、EXEC モードで **show mac address-table vlan** コマンドを使用します。

```
show mac address-table vlan vlan-id
```

| 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。  |      |      |           |                 |
|-----------|---|------|------|-----------|-----------------|
| デフォルト     | なし  |      |      |           |                 |
| コマンド モード  | EXEC  |      |      |           |                 |
| コマンド履歴    | <table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>15.0(1)EY</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 15.0(1)EY | このコマンドが導入されました。 |
| リリース      | 変更内容  |      |      |           |                 |
| 15.0(1)EY | このコマンドが導入されました。   |      |      |           |                 |

**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
```

## ■ show mac address-table vlan

## 関連コマンド

| コマンド   | 説明   |
|--|--|
| <code>show mac address-table address</code>      | 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。               |
| <code>show mac address-table aging-time</code>   | 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。            |
| <code>show mac address-table count</code>        | 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。          |
| <code>show mac address-table dynamic</code>      | 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。                   |
| <code>show mac address-table interface</code>    | 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。                |
| <code>show mac address-table notification</code> | 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。 |
| <code>show mac address-table static</code>       | スタティック MAC アドレス テーブル エントリだけを表示します。                   |

# show mls qos

Quality of Service (QoS) のグローバルな設定情報を表示するには、EXEC モードで **show mls qos** コマンドを使用します。

## show mls qos



(注) このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

### 構文の説明

このコマンドにはキーワードまたは引数はありません。

### デフォルト

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

### 例

次の例では、QoS がイネーブルで DSCP 透過もイネーブルの場合の **show mls qos** コマンドの出力を示します。

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

### 関連コマンド

| コマンド                    | 説明                         |
|-------------------------|----------------------------|
| <a href="#">mls qos</a> | スイッチ全体に対して QoS をイネーブルにします。 |

# show mls qos aggregate-policer

Quality of Service (QoS) の集約ポリサー設定を表示するには、EXEC モードで **show mls qos aggregate-policer** コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。

**show mls qos aggregate-policer** [*aggregate-policer-name*]



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

*aggregate-policer-name* (任意) 指定された名前のポリサー設定。

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show mls qos aggregate-policer** コマンドの出力を示します。

```
Switch> show mls qos aggregate-policer policer1
aggregate-policer policer1 1000000 2000000 exceed-action drop
Not used by any policy map
```

## 関連コマンド

| コマンド                                      | 説明                                     |
|---|--|
| <a href="#">mls qos aggregate-policer</a> | ポリシー マップ内で複数のクラスが共有するポリサー パラメータを定義します。 |

# show mls qos input-queue

入力キューの Quality of Service (QoS) の設定を表示するには、EXEC モードで **show mls qos input-queue** コマンドを使用します。

## show mls qos input-queue



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

### 構文の説明

このコマンドには、キーワードと引数はありません。

### デフォルト

なし

### コマンドモード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

### 例

次の例では、**show mls qos input-queue** コマンドの出力を示します。

```
Switch> show mls qos input-queue
Queue      :      1      2
-----
buffers    :      90     10
bandwidth  :       4      4
priority   :       0     10
threshold1 :     100    100
threshold2 :     100    100
```

### 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">mls qos srr-queue input bandwidth</a> | シェイプド ラウンドロビン (SRR) の重みを入力キューに割り当てます。                                       |
| <a href="#">mls qos srr-queue input buffers</a>   | 入力キュー間のバッファを割り当てます。   |
| <a href="#">mls qos srr-queue input cos-map</a>   | 割り当てられたサービス クラス (CoS) 値を入力キューにマッピングし、CoS 値をキューとしきい値 ID に割り当てます。             |
| <a href="#">mls qos srr-queue input dscp-map</a>  | 割り当てられた Diffserv コード ポイント (DSCP) 値を入力キューにマッピングし、DSCP 値をキューとしきい値 ID に割り当てます。 |

## ■ show mls qos input-queue

| コマンド  | 説明  |
|---|---|
| <code>mls qos srr-queue input priority-queue</code> | 入力プライオリティ キューを設定し、帯域幅を保証します。                        |
| <code>mls qos srr-queue input threshold</code>      | Weighted Tail-Drop (WTD) しきい値のパーセンテージを入力キューに割り当てます。 |

# show mls qos interface

ポート レベルで Quality of Service (QoS) の情報を表示するには、EXEC モードで **show mls qos interface** コマンドを使用します。

**show mls qos interface** [*interface-id*] [**buffers** | **queueing** | **statistics**]



(注) このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                     |  |
|---------------------|--|
| <i>interface-id</i> | (任意) 指定されたポート。有効なインターフェイスには、物理ポートが含まれます。   |
| <b>buffers</b>      | (任意) キュー間のバッファ割り当てを表示します。  |
| <b>queueing</b>     | (任意) キューイングの指針 (共有またはシェーピング) およびキューに対応したウェイトを表示します。  |
| <b>statistics</b>   | (任意) 送受信された DiffServ コード ポイント (DSCP) の統計情報、サービスクラス (CoS) 値、キューに入れられたかまたは出力キュー単位で削除されたパケット数、各ポリサーのプロファイル内外のパケット数を表示します。 |



(注) **policer** 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

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、VLAN ベース QoS がイネーブルの場合の **show mls qos interface interface-id** コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet1/1
GigabitEthernet1/1
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
```

## ■ show mls qos interface

```
qos mode:vlan-based
```

次の例では、VLAN ベース QoS がディセーブルの場合の **show mls qos interface interface-id** コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet1/2
GigabitEthernet1/2
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:port-based
```

次の例では、**show mls qos interface interface-id buffers** コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet1/2 buffers
GigabitEthernet1/2
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

次の例では、**show mls qos interface interface-id queueing** コマンドの出力を示します。出力緊急キューは、設定されたシェイプド ラウンドロビン (SRR) の重みを無効にします。

```
Switch> show mls qos interface gigabitethernet1/2 queueing
GigabitEthernet1/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) : 25 0 0 0
Shared queue weights : 25 25 25 25
The port bandwidth limit : 100 (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

次の例では、**show mls qos interface interface-id statistics** コマンドの出力を示します。表 2-30 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show mls qos interface gigabitethernet1/2 statistics
GigabitEthernet1/2

dscp: incoming
-----
 0 - 4 :      4213          0          0          0          0
 5 - 9 :         0          0          0          0          0
10 - 14 :        0          0          0          0          0
15 - 19 :        0          0          0          0          0
20 - 24 :        0          0          0          0          0
25 - 29 :        0          0          0          0          0
30 - 34 :        0          0          0          0          0
35 - 39 :        0          0          0          0          0
40 - 44 :        0          0          0          0          0
45 - 49 :        0          0          0          6          0
50 - 54 :        0          0          0          0          0
55 - 59 :        0          0          0          0          0
60 - 64 :        0          0          0          0          0
dscp: outgoing
-----
 0 - 4 :    363949          0          0          0          0
 5 - 9 :         0          0          0          0          0
10 - 14 :        0          0          0          0          0
15 - 19 :        0          0          0          0          0
20 - 24 :        0          0          0          0          0
```

```

25 - 29 :      0      0      0      0      0
30 - 34 :      0      0      0      0      0
35 - 39 :      0      0      0      0      0
40 - 44 :      0      0      0      0      0
45 - 49 :      0      0      0      0      0
50 - 54 :      0      0      0      0      0
55 - 59 :      0      0      0      0      0
60 - 64 :      0      0      0      0      0
cos: incoming
-----
0 - 4 :    132067      0      0      0      0
5 - 9 :      0      0      0      0      0
cos: outgoing
-----
0 - 4 :    739155      0      0      0      0
5 - 9 :      90      0      0      0      0

Policer: Inprofile:      0 OutofProfile:      0

```

表 2-30 show mls qos interface statistics のフィールドの説明

| フィールド   |              | 説明                  |
|---------|--------------|---------------------|
| DSCP    | incoming     | DSCP 値ごとに受信したパケット数  |
|         | outgoing     | DSCP 値ごとに送信したパケット数  |
| CoS     | incoming     | CoS 値ごとに受信したパケット数   |
|         | outgoing     | CoS 値ごとに送信したパケット数   |
| Policer | Inprofile    | ポリサーごとのプロファイル内パケット数 |
|         | OutofProfile | ポリサーごとのプロファイル外パケット数 |

## 関連コマンド

| コマンド   | 説明   |
|--|--|
| <a href="#">mls qos queue-set output buffers</a>       | バッファをキューセットに割り当てます。  |
| <a href="#">mls qos queue-set output threshold</a>     | Weighted Tail-Drop (WTD) しきい値を設定し、バッファのアービタリリティを保証し、キューセットに対する最大メモリ割り当てを設定します。 |
| <a href="#">mls qos srr-queue input bandwidth</a>      | SRR の重みを入力キューに割り当てます。  |
| <a href="#">mls qos srr-queue input buffers</a>        | 入力キュー間のバッファを割り当てます。  |
| <a href="#">mls qos srr-queue input cos-map</a>        | CoS 値を入力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングします。                          |
| <a href="#">mls qos srr-queue input dscp-map</a>       | DSCP 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングします。                        |
| <a href="#">mls qos srr-queue input priority-queue</a> | 入力プライオリティ キューを設定し、帯域幅を保証します。   |
| <a href="#">mls qos srr-queue input threshold</a>      | WTD しきい値のパーセンテージを入力キューに割り当てます。   |
| <a href="#">mls qos srr-queue output cos-map</a>       | CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。                           |
| <a href="#">mls qos srr-queue output dscp-map</a>      | DSCP 値を出力キュー、またはキューとしきい値 ID にマッピングします。   |
| <a href="#">policy-map</a>                             | ポリシー マップを作成、または変更します。  |

| コマンド                                   | 説明  |
|--|---|
| <code>priority-queue</code>            | ポート上で出力緊急キューをイネーブルにします。                                       |
| <code>queue-set</code>                 | ポートをキューセットにマッピングします。  |
| <code>srr-queue bandwidth limit</code> | ポートでの最大出力を制限します。  |
| <code>srr-queue bandwidth shape</code> | シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。 |
| <code>srr-queue bandwidth share</code> | 共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。         |

# show mls qos maps

Quality of Service (QoS) マッピング情報を表示するには、EXEC モードで **show mls qos maps** コマンドを使用します。分類では、QoS はマッピング テーブルを使用してトラフィックのプライオリティを表示し、受信したサービス クラス (CoS)、Diffserv コード ポイント (DSCP)、または IP precedence 値から対応する CoS または DSCP 値を取得します。

```
show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q |
dscp-mutation dscp-mutation-name | dscp-output-q | ip-prec-dscp | policed-dscp]
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <b>cos-dscp</b>                                | (任意) サービス クラス (CoS) /DSCP マップを表示します。        |
| <b>cos-input-q</b>                             | (任意) CoS 入力キューのしきい値マップを表示します。               |
| <b>cos-output-q</b>                            | (任意) CoS 出力キューのしきい値マップを表示します。               |
| <b>dscp-cos</b>                                | (任意) DSCP-to-CoS マップを表示します。                 |
| <b>dscp-input-q</b>                            | (任意) DSCP 入力キューしきい値マップを表示します。               |
| <b>dscp-mutation</b> <i>dscp-mutation-name</i> | (任意) 指定された DSCP-to-DSCP-mutation マップを表示します。 |
| <b>dscp-output-q</b>                           | (任意) DSCP 出力キューしきい値マップを表示します。               |
| <b>ip-prec-dscp</b>                            | (任意) IP precedence/DSCP マップを表示します。          |
| <b>policed-dscp</b>                            | (任意) ポリシング済み DSCP マップを表示します。                |

## デフォルト

なし

## コマンド モード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

ポリシング設定 DSCP、DSCP/CoS、および DSCP/DSCP-mutation マップは、マトリクスとして表示されます。d1 列では、DSCP で最も重要度の高い桁を指定します。d2 行では、DSCP で最も重要度の低い桁を指定します。d1 値および d2 値の共通部分では、ポリシング設定 DSCP、CoS、または Mutated-DSCP 値を提供します。たとえば、DSCP/CoS マップでは、DSCP 値 43 は CoS 値 5 に対応します。

DSCP 入力キューしきい値および DSCP 出力キューしきい値マップは、マトリクスとして表示されま  
す。d1 列では、最も重要度の高い DSCP 番号の桁を指定します。d2 行では、最も重要度の低い DSCP  
番号の桁を指定します。d1 値と d2 値の共通部分では、キュー ID としきい値 ID を提供します。たとえ  
ば、DSCP 入力キューしきい値マップでは、DSCP 値 43 はキュー 2 およびしきい値 1 (02-01) に対応  
します。

CoS 入力キューしきい値および CoS 出力キューしきい値マップでは、CoS 値が一番上の行、対応する  
キュー ID およびしきい値 ID が 2 番目の行に表示されます。たとえば、CoS 入力キューしきい値マッ  
プでは、CoS 値 5 はキュー 2 およびしきい値 1 (2-1) に対応することになります。

例 次の例では、**show mls qos maps** コマンドの出力を示します。

```
Switch> show mls qos maps
Policed-dscp map:
  d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
  0 :   00 01 02 03 04 05 06 07 08 09
  1 :   10 11 12 13 14 15 16 17 18 19
  2 :   20 21 22 23 24 25 26 27 28 29
  3 :   30 31 32 33 34 35 36 37 38 39
  4 :   40 41 42 43 44 45 46 47 48 49
  5 :   50 51 52 53 54 55 56 57 58 59
  6 :   60 61 62 63

Dscp-cos map:
  d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
  0 :   00 00 00 00 00 00 00 00 01 01
  1 :   01 01 01 01 01 01 02 02 02 02
  2 :   02 02 02 02 03 03 03 03 03 03
  3 :   03 03 04 04 04 04 04 04 04 04
  4 :   05 05 05 05 05 05 05 05 06 06
  5 :   06 06 06 06 06 06 07 07 07 07
  6 :   07 07 07 07

Cos-dscp map:
  cos:  0  1  2  3  4  5  6  7
-----
  dscp:  0  8 16 24 32 40 48 56

IpPrecedence-dscp map:
  ipprec:  0  1  2  3  4  5  6  7
-----
  dscp:  0  8 16 24 32 40 48 56

Dscp-outputq-threshold map:
  d1 :d2  0  1  2  3  4  5  6  7  8  9
-----
  0 :   02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
  1 :   02-01 02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01
  2 :   03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
  3 :   03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
  4 :   01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01
  5 :   04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
  6 :   04-01 04-01 04-01 04-01
```

```

Dscp-inputq-threshold map:
d1 :d2  0    1    2    3    4    5    6    7    8    9
-----
0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
2 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
3 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01
5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
6 :    01-01 01-01 01-01 01-01

Cos-outputq-threshold map:
      cos:  0    1    2    3    4    5    6    7
-----
queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1

Cos-inputq-threshold map:
      cos:  0    1    2    3    4    5    6    7
-----
queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1

Dscp-dscp mutation map:
Default DSCP Mutation Map:
d1 : d2  0    1    2    3    4    5    6    7    8    9
-----
0 :    00 01 02 03 04 05 06 07 08 09
1 :    10 11 12 13 14 15 16 17 18 19
2 :    20 21 22 23 24 25 26 27 28 29
3 :    30 31 32 33 34 35 36 37 38 39
4 :    40 41 42 43 44 45 46 47 48 49
5 :    50 51 52 53 54 55 56 57 58 59
6 :    60 61 62 63

```

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">mls qos map</a>                       | CoS/DSCP マップ、DSCP/CoS マップ、DSCP/DSCP-mutation マップ、IP precedence/DSCP マップ、およびポリシング設定 DSCP マップを定義します。 |
| <a href="#">mls qos srr-queue input cos-map</a>   | CoS 値を入力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングします。  |
| <a href="#">mls qos srr-queue input dscp-map</a>  | DSCP 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングします。  |
| <a href="#">mls qos srr-queue output cos-map</a>  | CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。   |
| <a href="#">mls qos srr-queue output dscp-map</a> | DSCP 値を出力キュー、またはキューとしきい値 ID にマッピングします。   |

# show mls qos queue-set

出力キューの Quality of Service (QoS) の設定を表示するには、EXEC モードで **show mls qos queue-set** コマンドを使用します。

**show mls qos queue-set** [*qset-id*]



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

*qset-id* (任意) キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ~ 2 です。

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show mls qos queue-set** コマンドの出力を示します。

```
Switch> show mls qos queue-set
Queueset: 1
Queue   :      1      2      3      4
-----
buffers  :      25      25      25      25
threshold1:    100    200    100    100
threshold2:    100    200    100    100
reserved  :      50      50      50      50
maximum   :      400     400     400     400
Queueset: 2
Queue   :      1      2      3      4
-----
buffers  :      25      25      25      25
threshold1:    100    200    100    100
threshold2:    100    200    100    100
reserved  :      50      50      50      50
maximum   :      400     400     400     400
```

## 関連コマンド

| コマンド   | 説明   |
|--|--|
| <a href="#">mls qos queue-set output buffers</a>   | バッファをキューセットに割り当てます。  |
| <a href="#">mls qos queue-set output threshold</a> | Weighted Tail-Drop (WTD) しきい値を設定し、バッファの<br>アベイラビリティを保証し、キューセットに対する最大メモ<br>リ割り当てを設定します。 |

# show mls qos vlan

スイッチ仮想インターフェイス (SVI) に付加されたポリシー マップを表示するには、EXEC モードで **show mls qos vlan** コマンドを使用します。

```
show mls qos vlan vlan-id
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                |   |
|----------------|---|
| <i>vlan-id</i> | ポリシー マップを表示するために SVI の VLAN ID を指定します。指定できる範囲は 1 ~ 4094 です。 |
|----------------|---|

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**show mls qos vlan** コマンドからの出力は、VLAN ベースの Quality of Service (QoS) がイネーブルで階層ポリシー マップが設定されている場合にだけ意味があります。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show mls qos vlan** コマンドの出力を示します。

```
Switch> show mls qos vlan 10
Vlan10
Attached policy-map for Ingress:pm-test-pm-2
```

## 関連コマンド

| コマンド                       | 説明  |
|----------------------------|---|
| <a href="#">policy-map</a> | 複数のポートに適用できるポリシー マップを作成または変更し、ポリシー マップ コンフィギュレーション モードを開始します。 |

# show monitor

スイッチ上のすべてのスイッチドポートアナライザ (SPAN) およびリモート SPAN (RSPAN) セッションに関する情報を表示するには、EXEC モードで **show monitor** 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]]
```

## 構文の説明

|                       |  |
|-----------------------|--|
| <b>session</b>        | (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。  |
| <b>all</b>            | すべての SPAN セッションを表示します。   |
| <b>local</b>          | ローカル SPAN セッションだけを表示します。   |
| <b>range list</b>     | 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す)。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。<br><br>(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。 |
| <b>remote</b>         | リモート SPAN セッションだけを表示します。   |
| <b>detail</b>         | (任意) 指定されたセッションの詳細情報を表示します。  |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 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 : Fa1/1
Both : Fa2/2-3,Fa2/5-6
Destination Ports : Fa1/2
Encapsulation : Replicate
Ingress : Disabled
```

```
Session 2
-----
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor EXEC** コマンドの出力を示します。

```
Switch# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Fa1/1
Both : Fa2/2-3,Fa2/5-6
Destination Ports : Fa2/8
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all 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 : Fa1/2
Destination Ports : Fa1/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
-----
Type : Local Session
Source Ports :
Both : Fa1/5
Destination Ports : Fa1/8
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

#### 関連コマンド

| コマンド                            | 説明                                |
|---------------------------------|-----------------------------------|
| <a href="#">monitor session</a> | SPAN または RSPAN セッションを開始、または修正します。 |

# show mvr

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) を含んだ、現在のマルチキャスト VLAN レジストレーション (MVR) のグローバルパラメータ値を表示するには、キーワードなしで特権 EXEC モードで **show mvr** コマンドを使用します。

## show mvr

### 構文の説明

このコマンドにはキーワードまたは引数はありません。

### デフォルト

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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 メンバー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  |
|--|---|
| <a href="#">mvr (グローバル コンフィギュレーション)</a>    | 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。  |
| <a href="#">mvr (インターフェイス コンフィギュレーション)</a> | MVR ポートを設定します。  |
| <a href="#">show mvr interface</a>         | コマンドに <b>interface</b> および <b>members</b> 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。 |
| <a href="#">show mvr members</a>           | 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

マルチキャスト VLAN レジストレーション (MVR) の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特権 EXEC モードで **show mvr interface** 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]]]
```

## 構文の説明

|                     |   |
|---------------------|---|
| <i>interface-id</i> | (任意) 指定したインターフェイス。<br>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。 |
| <b>members</b>      | (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。                           |
| <b>vlan vlan-id</b> | (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。         |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

入力したポートが非 MVR ポートまたは送信元ポートの場合は、エラーメッセージが戻されます。入力したポートがレシーバポートの場合は、ポートタイプ、ポート単位のステータス、および即時脱退設定が表示されます。

**members** キーワードを入力すると、インターフェイス上の MVR グループメンバがすべて表示されます。VLAN ID を入力すると、VLAN の MVR グループメンバがすべて表示されます。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface
Port          Type          Status          Immediate Leave
----          -
Gi1/1         SOURCE        ACTIVE/UP       DISABLED
Gi1/2         RECEIVER      ACTIVE/DOWN     DISABLED
```

上記の Status の定義は、次のとおりです。

- ACTIVE は、ポートが VLAN に含まれていることを意味します。
- UP/DOWN は、ポートが転送中か転送中でないかを示します。
- INACTIVE は、ポートが VLAN に含まれていないことを意味します。

## ■ show mvr interface

次の例では、指定されたポートの **show mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet1/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

次の例では、**show mvr interface interface-id members** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet1/2 members
239.255.0.0      DYNAMIC ACTIVE
239.255.0.1      DYNAMIC ACTIVE
239.255.0.2      DYNAMIC ACTIVE
239.255.0.3      DYNAMIC ACTIVE
239.255.0.4      DYNAMIC ACTIVE
239.255.0.5      DYNAMIC ACTIVE
239.255.0.6      DYNAMIC ACTIVE
239.255.0.7      DYNAMIC ACTIVE
239.255.0.8      DYNAMIC ACTIVE
239.255.0.9      DYNAMIC ACTIVE
```

## ■ 関連コマンド

| コマンド                              | 説明   |
|-----------------------------------|--|
| <b>mvr</b> (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。 |
| <b>mvr</b> (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。                               |
| <b>show mvr</b>                   | スイッチのグローバル MVR 設定を表示します。                     |
| <b>show mvr members</b>           | MVR マルチキャスト グループのメンバであるすべてのレシーバ ポートを表示します。   |

# show mvr members

現在 IP マルチキャスト グループのメンバであるすべてのレシーバおよび送信元ポートを表示するには、特権 EXEC モードで **show mvr members** コマンドを使用します。

**show mvr members** [*ip-address*]

## 構文の説明

*ip-address* (任意) IP マルチキャスト アドレスです。アドレスを入力すると、マルチキャスト グループのメンバであるすべてのレシーバおよび送信元ポートが表示されます。アドレスを入力しない場合は、すべての Multicast VLAN Registration (MVR) グループのすべてのメンバがリストされます。グループ内にメンバがない場合は、グループは **Inactive** として表示されます。

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**show mvr members** コマンドは、レシーバおよび送信元ポートに適用されます。MVR 互換モードの場合、すべての送信元ポートは、すべてのマルチキャスト グループのメンバです。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show mvr members** コマンドの出力を示します。

```
Switch# show mvr members
MVR Group IP      Status      Members
-----
239.255.0.1      ACTIVE      Gi1/1(d), Gi1/2(s)
239.255.0.2      INACTIVE    None
239.255.0.3      INACTIVE    None
239.255.0.4      INACTIVE    None
239.255.0.5      INACTIVE    None
239.255.0.6      INACTIVE    None
239.255.0.7      INACTIVE    None
239.255.0.8      INACTIVE    None
239.255.0.9      INACTIVE    None
239.255.0.10     INACTIVE    None
```

<output truncated>

次の例では、**show mvr members ip-address** コマンドの出力を示します。次のアドレスを持った IP マルチキャスト グループのメンバを表示します。

```
Switch# show mvr members 239.255.0.2
239.255.003.--22    ACTIVE      Gi1/1(d), Gi1/2(d), Gi1/3(d),
                  Gi1/4(d), Gi1/5(s)
```

## ■ show mvr members

| 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 <b>members</b> キーワードを追加した場合、設定された MVR インターフェイス、指定されたインターフェイスのステータス、またはインターフェイスが属するすべてのマルチキャストグループが表示されます。 |

# show network-policy profile

ネットワーク ポリシー プロファイルを表示するには、特権 EXEC モードで **show network policy profile** コマンドを使用します。

**show network-policy profile** [*profile number*] [*detail*]



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

## 構文の説明

|                       |  |
|-----------------------|--|
| <i>profile number</i> | (任意) ネットワーク ポリシー プロファイル番号を表示します。プロファイルが入力されていない場合、すべてのネットワーク ポリシー プロファイルが表示されます。 |
| <i>detail</i>         | (任意) 詳細なステータスおよび統計情報を表示します。  |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、**show network-policy profile** コマンドの出力を示します。

```
Switch# show network-policy profile
Network Policy Profile 10
  voice vlan 17 cos 4
  Interface:
  none
Network Policy Profile 30
  voice vlan 30 cos 5
  Interface:
  none
Network Policy Profile 36
  voice vlan 4 cos 3
  Interface:
  Interface_id
```

## 関連コマンド

| コマンド  | 説明                          |
|---|-----------------------------|
| <a href="#">network-policy</a>                                  | インターフェイスにネットワークポリシーを適用します。  |
| <a href="#">network-policy profile (グローバル コンフィギュレーション)</a>      | ネットワークポリシー プロファイルを作成します。    |
| <a href="#">network-policy profile (ネットワークポリシー コンフィギュレーション)</a> | ネットワークポリシー プロファイルの属性を設定します。 |

# show nmsp

スイッチのネットワーク モビリティ サービス プロトコル (NMSP) 情報を表示するには、特権 EXEC モードで **show nmsp** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。

```
show nmsp {attachment suppress interface | capability | notification interval | statistics
           {connection | summary} | status | subscription {detail | summary}}
```

## 構文の説明

|  |   |
|--|---|
| <b>attachment suppress interface</b>   | アタッチメント抑制インターフェイスを表示します。  |
| <b>capability</b>                      | サポートされるサービスとサブ サービスを含むスイッチ機能を表示します。   |
| <b>notification interval</b>           | サポートされるサービスの通知間隔を表示します。   |
| <b>statistics connection   summary</b> | NMSP の統計情報を表示します。 <ul style="list-style-type: none"> <li>• <b>connection</b> : 各接続でのメッセージ カウンタを表示します。</li> <li>• <b>summary</b> : グローバル カウンタを表示します。</li> </ul>  |
| <b>status</b>                          | NMSP 接続に関する情報を表示します。  |
| <b>subscription detail   summary</b>   | 各 NMSP 接続に関するサブスクリプション情報を表示します。 <ul style="list-style-type: none"> <li>• <b>detail</b> : 各接続でサブスクライブしているすべてのサービスとサブ サービスを表示します。</li> <li>• <b>summary</b> : 各接続でサブスクライブしているすべてのサービスを表示します。</li> </ul> |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、**show nmsp attachment suppress interface** コマンドの出力を示します。

```
Switch# show nmsp attachment suppress interface
NMSP Attachment Suppression Interfaces
-----
GigabitEthernet1/1
GigabitEthernet1/2
```

次の例では、**show nmosp capability** コマンドの出力を示します。

```
Switch# show nmosp capability
NMSP Switch Capability
-----
Service           Subservice
-----
Attachment        Wired Station
Location          Subscription
```

次の例では、**show nmosp notification interval** コマンドの出力を示します。

```
Switch# show nmosp notification interval
NMSP Notification Intervals
-----
Attachment notify interval: 30 sec (default)
Location notify interval: 30 sec (default)
```

次の例では、**show nmosp statistics connection** コマンドと **show nmosp statistics summary** コマンドの出力を示します。

```
Switch# show nmosp statistics connection
NMSP Connection Counters
-----
Connection 1:
  Connection status: UP
  Freed connection: 0

  Tx message count      Rx message count
  -----
  Subscr Resp: 1        Subscr Req: 1
  Capa Notif: 1         Capa Notif: 1
  Atta Resp: 1          Atta Req: 1
  Atta Notif: 0
  Loc Resp: 1           Loc Req: 1
  Loc Notif: 0
  Unsupported msg: 0

Switch# show nmosp statistics summary
NMSP Global Counters
-----
  Send too big msg: 0
  Failed socket write: 0
  Partial socket write: 0
  Socket write would block: 0
  Failed socket read: 0
  Socket read would block: 0
  Transmit Q full: 0
  Max Location Notify Msg: 0
  Max Attachment Notify Msg: 0
  Max Tx Q Size: 0
```

次の例では、**show nmosp status** コマンドの出力を示します。

```
Switch# show nmosp status
NMSP Status
-----
NMSP: enabled
MSE IP Address      TxEchoResp RxEchoReq TxData RxData
172.19.35.109      5 5 4 4
```

## ■ show nmosp

次の例では、**show nmosp show subscription detail** コマンドと **show nmosp show subscription summary** コマンドの出力を示します。

```
Switch# show nmosp subscription detail
Mobility Services Subscribed by 172.19.35.109:
Services                Subservices
-----                -
Attachment:            Wired Station
Location:              Subscription
```

```
Switch# show nmosp subscription summary
Mobility Services Subscribed:
MSE IP Address         Services
-----                -
172.19.35.109         Attachment, Location
```

## 関連コマンド

| コマンド                          | 説明   |
|-------------------------------|--|
| <b>clear nmosp statistics</b> | NMSP 統計カウンタをクリアします。                              |
| <b>nmosp</b>                  | スイッチ上でネットワーク モビリティ サービス プロトコル (NMSP) をイネーブルにします。 |

# 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、EXEC モードで **show pagp** コマンドを使用します。

**show pagp** [*channel-group-number*] {**counters** | **dual-active** | **internal** | **neighbor**}

| 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 ~ 6 です。 |
| <b>counters</b>             | トラフィック情報を表示します。                         |
| <b>dual-active</b>          | デュアル アクティブ ステータスを表示します。                 |
| <b>internal</b>             | 内部情報を表示します。                             |
| <b>neighbor</b>             | ネイバーの情報を表示します。                          |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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
Gi1/1     45    42      0      0
Gi1/2     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
Gi1/1     SC   U6/S7   H      30s     1     128   Any    16
```

## ■ show pagp

```
Gi1/2      SC      U6/S7      H      30s      1      128      Any      16
```

次の例では、**show pagp 1 neighbor** コマンドの出力を示します。

```
Switch> show pagp 1 neighbor
  Flags: S - Device is sending Slow hello.  C - Device is in Consistent state.
         A - Device is in Auto mode.        P - Device learns on physical port.

Channel group 1 neighbors
Port      Partner          Partner          Partner          Partner Group
Gi1/1     switch-p2       0002.4b29.4600  Gi0/1            9s SC          10001
Gi1/2     switch-p2       0002.4b29.4600  Gi0/2            24s SC         10001
```

次の例では、**show pagp dual-active** コマンドの出力を示します。

```
Switch> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
Port      Dual-Active      Partner          Partner          Partner
Gi1/1     Detect Capable  Name            Port            Version
Gi1/1     No              Switch          Gi1/3           N/A

<output truncated>
```

## 関連コマンド

| コマンド                       | 説明                        |
|----------------------------|---------------------------|
| <a href="#">clear pagp</a> | PAgP チャンネル グループ情報をクリアします。 |

# show parser macro

スイッチ上で設定されているすべてのマクロ、または1つのマクロのパラメータを表示するには、EXEC モードで **show parser macro** コマンドを使用します。

```
show parser macro [{brief | description [interface interface-id] | name word}]
```

## 構文の説明

|   |   |
|---|---|
| <b>brief</b>                              | (任意) 各マクロの名前を表示します。                     |
| <b>description interface interface-id</b> | (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。 |
| <b>name word</b>                          | (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。      |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。シスコ デフォルト マクロの出力は、スイッチのプラットフォームとスイッチ上で実行しているソフトウェア イメージによって異なります。

```
Switch# show parser macro
<output truncated>

Macro name : cisco-ie-global
Macro type : default global
#global macro name cisco-ie-global macro
#macro description cisco-ie-global
# Access List and Policy Map for CIP QoS
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any

class-map match-all CIP-Implicit_dscp_55
 match access-group 101
class-map match-all CIP-Implicit_dscp_47
 match access-group 102
class-map match-all CIP-Implicit_dscp_43
 match access-group 103
```

## show parser macro

```

class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Other
  match access-group 105
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all 1588-PTP-General
  match access-group 107
<output truncated>
-----
Macro name : cisco-ethernetip
Macro type : default interface
#macro keywords $access_vlan
#macro name cisco-ethernetip
#macro description cisco-ethernetip
switchport host
switchport access vlan $access_vlan
storm-control broadcast level 3.00 1.00
service-policy input CIP-PTP-Traffic
priority-queue out
srr-queue bandwidth share 1 19 40 40
<output truncated>
-----
Macro name : cisco-ie-desktop
Macro type : default interface
# macro keywords $access_vlan
#macro name cisco-ie-desktop
switchport mode access
switchport access vlan $access_vlan
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 2
switchport port-security violation restrict
no switchport port-security aging type inactivity
no switchport access vlan
no switchport mode access
no spanning-tree portfast
no spanning-tree bpduguard enable
no macro description
-----
Macro name : cisco-ie-switch
Macro type : default interface
# macro keywords $native_vlan
#macro name: cisco-ie-switch
switchport mode trunk
switchport trunk native vlan $native_vlan
spanning-tree link-type point-to-point
mls qos trust cos
service-policy input CIP-PTP-Traffic
priority-queue out
srr-queue bandwidth share 1 19 40 40
no macro description
macro description cisco-ie-switch
<output truncated>

```

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 standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed

```

```
channel-protocol pagp
```

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
<output truncated>
  default global      : cisco-ie-global
  default interface:  cisco-ethernetip
  default interface:  cisco-ie-desktop
  default interface:  cisco-ie-switch
  default interface:  cisco-ie-router
  default interface:  cisco-ie-phone
  default interface:  cisco-ie-wireless
Switch#
```

次の例では、**show parser macro description** コマンドの出力を示します。

```
Switch# show parser macro description
Global Macro(s): cisco-global
Interface      Macro Description(s)
-----
Gi1/1          standard-switch10
Gi1/2          this is test macro
-----
```

次の例では、**show parser description interface** コマンドの出力を示します。

```
Switch# show parser macro description interface gigabitethernet1/2
Interface      Macro Description
-----
Gi1/2          this is test macro
-----
```

## 関連コマンド

| コマンド                            | 説明  |
|---------------------------------|---|
| <b>macro apply</b>              | 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。  |
| <b>macro description</b>        | 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。   |
| <b>macro global</b>             | 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。  |
| <b>macro global description</b> | 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。   |
| <b>macro name</b>               | マクロを作成します。  |
| <b>show running-config</b>      | 定義されたマクロを含む現在の動作設定を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# show policy-map

着信トラフィックの分類基準を定義する Quality of Service (QoS) のポリシー マップを表示するには、EXEC モードで **show policy-map** コマンドを使用します。ポリシーマップには、帯域幅制限および制限を超過した場合の対処法を指定するポリサーを格納できます。

```
show policy-map [policy-map-name [class class-map-name]]
```

## 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。           |
| <b>class</b> <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。 |



(注)

**control-plane** および **interface** キーワードは、コマンドラインのヘルプ スtring には表示されませんが、サポートされていません。表示されている統計情報は無視してください。

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show policy-map** コマンドの出力を示します。

```
Switch> show policy-map
Policy Map videowizard_policy2
  class videowizard_10-10-10-10
    set dscp 34
    police 100000000 2000000 exceed-action drop

Policy Map mypolicy
  class dscp5
    set dscp 6
```

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

# 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、特権 EXEC モードで **show port-security** コマンドを使用します。

**show port-security [interface interface-id] [address | vlan]**

## 構文の説明

|                               |  |
|-------------------------------|--|
| <b>interface interface-id</b> | (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。 |
| <b>address</b>                | (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。                                  |
| <b>vlan</b>                   | (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。                                  |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show port-security** コマンドの出力を示します。

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr    SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
Gi1/1            1                0                0                Shutdown
-----
```

## ■ show port-security

```
Total Addresses in System (excluding one mac per port)      : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

次の例では、**show port-security interface interface-id** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet1/1
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

次の例では、**show port-security address** コマンドの出力を示します。

```
Switch# show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
        (mins)
-----
  1     0006.0700.0800  SecureConfigured   Gi1/2    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 gigabitethernet1/2 address** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet1/2 address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
        (mins)
-----
  1     0006.0700.0800  SecureConfigured   Gi1/2    1
-----
Total Addresses: 1
```

次の例では、**show port-security interface interface-id vlan** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet1/2 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   |
|--|--|
| <a href="#">clear port-security</a>      | 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。   |
| <a href="#">switchport port-security</a> | ポート上でポートセキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC アドレスを設定します。 |

# show power inline

指定された Power over Ethernet (PoE) ポートまたはすべての PoE ポートの PoE ステータスを表示するには、**show power inline** コマンドを EXEC モードで使用します。

**show power inline** [*interface-id* | **consumption**]

## 構文の説明

|                     |   |
|---------------------|---|
| <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。 |
| <b>consumption</b>  | (任意) PoE ポートに接続した装置に割り当てられる電力を表示します。    |

## コマンドモード

ユーザ EXEC  
特権 EXEC

## コマンド履歴

| リリース       | 変更内容            |
|------------|-----------------|
| 15.0(2)EY1 | 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ポート番号、管理（設定）ステータス、現在の（実際の）ステータス、消費電力、およびデバイス タイプ情報を表示するためにこのコマンドを使用します。

Output :

```

Available      Used      Remaining
(Watts)        (Watts)   (Watts)
-----
<65.0>         <0.0>    <65.0>
Interface      Admin Oper      Power   Device      Class Max
(Watts)
-----
Fa<M#>/<P#>  <Admin> <Oper>   <Power> <Device>   <Class> <Max>

```

Note: P# - Port Number

```

Total          - Total available power budget in watts
Used           - Utilized Power in watts
Remaining      - Remaining power in watts
Admin          - Admin status
Oper          - Operator status
Power         - Allocated power to Power Device (PD) in watts
Device        - Name of the Power Device (PD)
Class         - Class of Power Device (PD)
Max           - Maximum Power, PD can draw

```

## 例

次では、IE 2000 スイッチでの **show power inline** コマンドの出力例を示します。

IE 2000 スイッチは最大ワット数 30 ワットの PoE+ をサポートします。

```

Switch> show power inline
Available      Used      Remaining
(Watts)        (Watts)   (Watts)
-----
65.0           0.0      65.0
Interface      Admin Oper      Power   Device      Class Max
(Watts)

```

## ■ show power inline

```

-----
Fa1/1 auto off 0.0 n/a n/a 30.0
Fa1/3 auto off 0.0 n/a n/a 30.0
Fa1/5 auto off 0.0 n/a n/a 30.0
Fa1/7 auto off 0.0 n/a n/a 30.0

```

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">logging event power-inline-status</a> | PoE イベントのロギングをイネーブルにします。                   |
| <a href="#">power inline</a>                      | 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。 |
| <a href="#">show controllers power inline</a>     | 指定した PoE コントローラのレジスタ値を表示します。               |

# show profinet

スイッチの PROFINET セッションに関する情報を表示するには、EXEC モードで **show profinet** コマンドを使用します。

**show profinet {alarm | lldp | session | status}**

## 構文の説明

|                |                                     |
|----------------|-------------------------------------|
| <b>alarm</b>   | PROFINET アラームを表示します。                |
| <b>lldp</b>    | PROFINET リンク層検出プロトコル (LLDP) を表示します。 |
| <b>session</b> | PROFINET セッションを表示します。               |
| <b>status</b>  | PROFINET ステータスを表示します。               |

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

LLDP および PROFINET がイネーブルにされると、このコマンドで PROFINET 形式の LLDP パケットが送受信される物理ポートが表示されます。

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、PROFINET アラームを表示する方法を示します。

```
Switch> show profinet alarm
Monitoring of Profinet Switch Alarms
  RPS Alarm: -
  CF Alarm: -
  Primary Temperature Alarm: -
  Secondary Temperature Alarm: -
  Major Relay Alarm: -
  Minor Relay Alarm: -
Monitoring of Profinet Port Alarms
Port      Link Fault      Not Forwarding Not Operating  FCS Error
Fa1/1     -                -                -                -
Fa1/2     -                -                -                -
Fa1/3     -                -                -                -
Fa1/4     -                -                -                -
Fa1/5     -                -                -                -
Fa1/6     -                -                -                -
Fa1/7     -                -                -                -
Fa1/8     -                -                -                -
Gi1/1     -                -                -                -
Gi1/2     -                -                -                -
```

次の例では、PROFINET LLDP を表示する方法を示します。

## show profinet

```
Switch> show profinet lldp
Fa1/1 port-003 Off
Fa1/2 port-004 Off
Fa1/3 port-005 Off
Fa1/4 port-006 Off
Fa1/5 port-007 Off
Fa1/6 port-008 Off
Fa1/7 port-009 Off
Fa1/8 port-010 Off
Gi1/1 port-001 Off
Gi1/2 port-002 Off
Switch>
```

次の例では、PROFINET セッションを表示する方法を示します。

```
Switch> show profinet session
Session #1
-----
Connected: No
Number Of IO CR's: 0
Number Of DiffModules: 0
```

次の例では、PROFINET ステータスを表示する方法を示します。

```
Switch> show profinet status
State      : Enabled
Vlan       : 1
Id         : IE2000-8TC
Connected  : Yes
ReductRatio : 512
GSD version : Match
```

## 関連コマンド

| コマンド                                    | 説明  |
|---|---|
| <a href="#">debug profinet alarm</a>    | PROFINET アラームのデバッグをイネーブルにします。   |
| <a href="#">debug profinet cyclic</a>   | PROFINET 巡回パケットの送受信に関連するファンクション コールを表示します。  |
| <a href="#">debug profinet error</a>    | PROFINET セッション エラーのデバッグをイネーブルにします。  |
| <a href="#">debug profinet packet</a>   | PROFINET パケットのデバッグをイネーブルにします。   |
| <a href="#">debug profinet platform</a> | Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにします。  |
| <a href="#">debug profinet topology</a> | 受信した PROFINET トポロジ パケットを表示します。  |
| <a href="#">debug profinet trace</a>    | トレースした一連のデバッグ出力ログを表示します。  |
| <a href="#">profinet</a>                | スイッチの PROFINET 機能をイネーブルにします。  |
| <a href="#">show debugging</a>          | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# show psp config

VLAN 上の特定のプロトコルに対して設定されているプロトコル ストーム プロテクションのステータスを表示するには、特権 EXEC モードで **show psp config** コマンドを使用します。

**show psp config {arp | dhcp | igmp}**

| 構文の説明 | arp  | dhcp   | igmp   |
|-------|--|--|--|
|       | ARP および ARP スヌーピングのプロトコル ストーム プロテクション ステータスを表示します。 | DHCP および DHCP スヌーピングのプロトコル ストーム プロテクション ステータスを表示します。 | IGMP および IGMP スヌーピングのプロトコル ストーム プロテクション ステータスを表示します。 |

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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

例 次の例では、**show psp config dhcp** コマンドの出力を示します。受信速度が 1 秒間に 35 パケットを超えた場合にパケットをドロップするようにプロトコル ストーム プロテクションが設定されています。

```
Switch# show psp config dhcp

-----
PSP Protocol Configuration Summary:
-----

DHCP Rate Limit      : 35 packets/sec
PSP Action           : Packet Drop
```

| 関連コマンド | コマンド                                     | 説明   |
|--------|--|--|
|        | <b>clear psp counter</b>                 | ドロップされたパケットのカウンタをクリアします。                           |
|        | <b>psp {arp   dhcp   igmp} pps value</b> | ARP、DHCP、または IGMP のプロトコル ストーム プロテクションを設定します。       |
|        | <b>show psp statistics</b>               | プロトコル ストーム プロテクションが設定されている場合に、ドロップされたパケットの数を表示します。 |

# show psp statistics

プロトコル ストーム プロテクションが設定されている場合に、すべてのプロトコルについてドロップされたパケットの数を表示するには、特権 EXEC モードで **show psp statistics** コマンドを使用します。

**show psp statistics [arp | dhcp | igmp]**

## 構文の説明

|             |  |
|-------------|--|
| <b>arp</b>  | (任意) ARP および ARP スヌーピングのドロップされたパケットの数を表示します。   |
| <b>dhcp</b> | (任意) DHCP および DHCP スヌーピングのドロップされたパケットの数を表示します。 |
| <b>igmp</b> | (任意) IGMP および IGMP スヌーピングのドロップされたパケットの数を表示します。 |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、DHCP に対してプロトコル ストーム プロテクションが設定されている場合の **show psp statistics dhcp** コマンドの出力を示します。出力では、13 個のパケットがドロップされたことが示されています。

```
Switch# show psp statistics dhcp

-----
PSP Protocol Drop Counter Summary:
-----
DHCP Drop Counter: 13
```

## 関連コマンド

| コマンド                                     | 説明   |
|--|--|
| <b>clear psp counter</b>                 | ドロップされたパケットのカウンタをクリアします。                     |
| <b>psp {arp   dhcp   igmp} pps value</b> | ARP、DHCP、または IGMP のプロトコル ストーム プロテクションを設定します。 |
| <b>show psp config</b>                   | プロトコル ストーム プロテクションの設定を表示します。                 |

# show ptp

グローバル高精度時間プロトコル (PTP) プロパティを表示します。特権 EXEC モードで **show ptp** コマンドを使用します。

**show ptp {clock | foreign-master-record | parent | time-property}**

## 構文の説明

|                              |                           |
|------------------------------|---------------------------|
| <b>clock</b>                 | PTP クロック プロパティを表示します。     |
| <b>foreign-master-record</b> | 外部マスター データ セットを表示します。     |
| <b>parent</b>                | 親およびグランドマスター プロパティを表示します。 |
| <b>time-property</b>         | PTP 時間プロパティを表示します。        |

## デフォルト

なし

## コマンドデフォルト

デフォルト設定はありません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**show ptp foreign-master-record** コマンドは、エンドツーエンド トランスペアレント モードにある場合でも境界クロック モードに適用されます。

スイッチが PTP フォワード モードの場合、**show ptp clock** または **show ptp port** 特権 EXEC コマンドを入力すると、情報が使用できないことを示すエラー メッセージが表示されます。

## 例

次の例では、**show ptp clock** コマンドの出力を示します。

```
Switch# show ptp clock
PTP CLOCK INFO
  PTP Device Type: Boundary clock
  Clock Identity: 0x0:9:B7:FF:FE:FF:F3:0
  Clock Domain: 0
  Number of PTP ports: 10
  Priority1: 128
  Priority2: 128
  Clock Quality:
    Class: 248
    Accuracy: Unknown
    Offset (log variance): N/A
  Offset From Master: 0
  Mean Path Delay: 490
  Steps Removed: 1
  Local clock time: 18:49:38 UTC Mar 7 1993
```

## show ptp

次の例では、**show ptp parent** コマンドの出力を示します。

```
Switch# show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
    Parent Clock Identity: 0x0:1E:13:FF:FE:0:28:0
    Parent Port Number: 1
    Observed Parent Offset (log variance): N/A
    Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
    Grandmaster Clock Identity: 0x0:1E:13:FF:FE:0:28:0
    Grandmaster Clock Quality:
      Class: 248
      Accuracy: Unknown
      Offset (log variance): N/A
      Priority1: 127
      Priority2: 128
```

次の例では、**show ptp time-property** コマンドの出力を示します。

```
Switch# show ptp time-property
PTP CLOCK TIME PROPERTY:
  Current UTC Offset valid: 0
  Current UTC Offset: 0
  Leap59: 0
  Leap61: 0
  Time Traceable: 16
  Frequency Traceable: 32
  PTP Timescale: 1
  Time Source: Internal Oscillator
```

次の例では、**show ptp foreign-master-record** コマンドの出力を示します。

```
Switch# show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
Interface FastEthernet1/1
  Foreign Master Clock Identity: FF:EE:DD:FF:FE:CC:BB:AA
  Foreign Master Port Number: 4
  Number of Announce Messages: 3
  Message Received Port: 1
  Most Recent Time stamps: 73097688078005270, 73097687836293940
Interface FastEthernet1/2
  Empty
Interface FastEthernet1/3
  Empty
Interface FastEthernet1/4
  Empty
Interface GigabitEthernet1/1
  Empty
Interface GigabitEthernet1/2
  Foreign Master Clock Identity: 00:09:B7:FF:FE:FF:7D:80
  Foreign Master Port Num: 6
  Number of Announce messages: 3
  Message received port: 6
  Most Recent Time stamps: 73097687967991270, 73097687725402960
```

## 関連コマンド

| コマンド                           | 説明                          |
|--------------------------------|-----------------------------|
| <b>debug ptp</b>               | PTP アクティビティのデバッグをイネーブルにします。 |
| <b>ptp (グローバル コンフィギュレーション)</b> | グローバル PTP クロック プロパティを設定します。 |

| コマンド                                    | 説明                              |
|---|---------------------------------|
| <code>ptp</code> (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 PTP クロック プロパティを設定します。 |
| <code>show ptp port</code>              | ポートの PTP プロパティを表示します。           |

# show ptp port

Precision Time Protocol (PTP) ポート プロパティを表示します。特権 EXEC モードで **show ptp port** コマンドを使用します。

**show ptp port** [**FastEthernet interface**| **GigabitEthernet interface**]

## 構文の説明

|                                  |  |
|----------------------------------|--|
| <b>FastEthernet interface</b>    | (任意) 指定されたポートの PTP FastEthernet プロパティを表示します。     |
| <b>GigabitEthernet interface</b> | (任意) 指定されたポートの PTP Gigabit Ethernet プロパティを表示します。 |

## デフォルト

なし

## コマンドデフォルト

デフォルト設定はありません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 例

次の例では、**show ptp port FastEthernet 1/1** コマンドの出力を示します。

```
Switch# show ptp port FastEthernet 1/1
PTP PORT DATASET: FastEthernet1/1
  Port identity: clock identity: 0x0:9:B7:FF:FE:FF:F3:0
  Port identity: port number: 1
  PTP version: 2
  Port state: SLAVE
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay: 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 50000
```

## 関連コマンド

| コマンド                                       | 説明                          |
|--|-----------------------------|
| <a href="#">ptp (インターフェイス コンフィギュレーション)</a> | PTP クロック プロパティを設定します。       |
| <a href="#">show ptp</a>                   | ポートの PTP クロック プロパティを設定します。  |
| <a href="#">debug ptp</a>                  | PTP アクティビティのデバッグをイネーブルにします。 |

# show rep topology

セグメント、またはセグメント内のプライマリおよびセカンダリ エッジ ポートを含むすべてのセグメントの Resilient Ethernet Protocol (REP) トポロジ情報を表示するには、EXEC モードで **show rep topology** コマンドを使用します。

**show rep topology** [*segment segment\_id*] [*archive*] [*detail*]

| 構文の説明 | segment<br><i>segment-id</i> | (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。 |
|-------|------------------------------|---|
|       | <b>archive</b>               | (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。   |
|       | <b>detail</b>                | (任意) REP トポロジの詳細情報を表示します。                                   |

デフォルト なし

コマンド モード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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 次の例では、**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_3400 Gi1/13              Open
sw3_multseg_3400 Gi1/14              Alt
sw4_multseg_3400 Gi0/13              Open
sw4_multseg_3400 Gi0/14              Open
sw5_multseg_3400 Gi1/13              Open
sw5_multseg_3400 Gi1/14              Open
sw2_multseg_3750 Gi1/0/2              Open
sw2_multseg_3750 Gi1/0/1              Open
sw1_multseg_3750 Gi1/0/2      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。

## ■ show rep topology

```
Switch # show rep topology
REP Segment 2
BridgeName      PortName      Edge  Role
-----
sw8-ts8-51      Gil/2          Pri*  Open
sw9-ts11-50     Gil/0/4        Open
sw9-ts11-50     Gil/0/2        Open
sw1-ts11-45     Gi0/2          Alt
sw1-ts11-45     Po1            Open
sw8-ts8-51      Gil/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, Gil/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 Gil/1/1        Pri  Open
sw3_multseg_3400 Gil/13         Open
sw3_multseg_3400 Gil/14         Open
sw4_multseg_3400 Gil/13         Open
sw4_multseg_3400 Gil/14         Open
sw5_multseg_3400 Gil/13         Open
sw5_multseg_3400 Gil/14         Open
sw2_multseg_3750 Gil/1/2        Alt
sw2_multseg_3750 Gil/1/1        Open
sw1_multseg_3750 Gil/1/2        Sec  Open
```

## 関連コマンド

| コマンド                        | 説明  |
|-----------------------------|---|
| <a href="#">rep segment</a> | 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 sdm prefer

特定の機能にシステム リソースを最大限割り当てるために使用可能な Switch Database Management (SDM) テンプレートに関する情報を表示するには、特権 EXEC モードで **show sdm prefer** コマンドを使用します。

**show sdm prefer [default | dual-ipv4-and-ipv6 {default | routing} qos | routing]**

## 構文の説明

|   |   |
|---|---|
| <b>default</b>                              | (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。   |
| <b>dual-ipv4-and-ipv6 default   routing</b> | (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"> <li>• <b>default</b> : デフォルトのデュアル テンプレート設定を表示します。</li> <li>• <b>routing</b> : 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。</li> </ul> |
| <b>qos</b>                                  | (任意) Quality of Service (QoS) アクセス コントロール エントリ (ACE) 用のシステム リソースを最大化するテンプレートを表示します。   |
| <b>routing</b>                              | (任意) IPv4 ルーティング用のシステム リソースを最大化するテンプレートを表示します。  |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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** コマンドを入力した場合、**show sdm prefer** により、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

各テンプレートで表示される番号は、各機能のリソースにおけるおおよその最大数になります。他に設定された機能の実際の数字にもよるため、実際の数字とは異なる場合があります。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次に、**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:                12K
```

```

number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes: 0
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.75K
number of IPv4/MAC security aces: 1K

```

次に、**show sdm prefer dual-ipv4-and-ipv6** コマンドの出力例を示します。

```

Switch# show sdm prefer qos
"qos" template:
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 8K
number of IPv4 IGMP groups: 0.25K
number of IPv4/MAC qos aces: 0.625k
number of IPv4/MAC security aces: 0.125k

```

次に、**show sdm prefer routing** コマンドの出力例を示します。

```

Switch# show sdm prefer routing
"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: 2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes: 4K
  number of directly-connected IPv4 hosts: 2K
  number of indirect IPv4 routes: 2K
number of IPv4 policy based routing aces: 0.5K
number of IPv4/MAC qos aces: 0.625k
number of IPv4/MAC security aces: 0.375k

```

次の例では、**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
"dual-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: 1K
number of IPv4 IGMP groups + multicast routes: 0.5K
number of IPv4 unicast routes: 2K
  number of directly-connected IPv4 hosts: 1K
  number of indirect IPv4 routes: 1K
number of IPv6 multicast groups: 0.625k
number of directly-connected IPv6 addresses: 1K
number of indirect IPv6 unicast routes: 0.375k
number of IPv4 policy based routing aces: 0.125k
number of IPv4/MAC qos aces: 0.375k
number of IPv4/MAC security aces: 0.125k
number of IPv6 policy based routing aces: 0.125k
number of IPv6 qos aces: 0.125k
number of IPv6 security aces: 0.125k

```

#### 関連コマンド

| コマンド                       | 説明                            |
|----------------------------|-------------------------------|
| <a href="#">sdm prefer</a> | SDM テンプレートを最大化されたリソース量に設定します。 |

# show setup express

Express Setup モードがスイッチでアクティブかどうかを表示するには、特権 EXEC モードで **show setup express** コマンドを使用します。

## show setup express

### 構文の説明

このコマンドには、引数またはキーワードはありません。

### デフォルト

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 例

次の例は、**show setup express** コマンドの出力を示しています。

```
Switch# show setup express
express setup mode is active
```

### 関連コマンド

| コマンド                          | 説明                           |
|-------------------------------|------------------------------|
| <a href="#">setup express</a> | Express Setup モードをイネーブルにします。 |

# show spanning-tree

スパニング ツリー ステータス情報を表示するには、EXEC モードで **show spanning-tree** コマンドを使用します。

```
show spanning-tree [bridge-group | active [detail] | backbonefast | blockedports | bridge | detail
[active] | inconsistentports | interface interface-id | mst | pathcost method | root | summary
[totals] | uplinkfast | vlan vlan-id]
```

```
show spanning-tree bridge-group [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary]
```

```
show spanning-tree vlan vlan-id [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary]
```

```
show spanning-tree {vlan vlan-id | bridge-group} bridge [address | detail | forward-time |
hello-time | id | max-age | priority [system-id] | protocol ]
```

```
show spanning-tree {vlan vlan-id | bridge-group} root [address | cost | detail | forward-time |
hello-time | id | max-age | port | priority [system-id] ]
```

```
show spanning-tree interface interface-id [active [detail] | cost | detail [active] | inconsistency |
portfast | priority | rootcost | state]
```

```
show spanning-tree mst [configuration [digest]] | [instance-id [detail | interface interface-id
[detail]]]
```

## 構文の説明

|  |  |
|--|--|
| <i>bridge-group</i>  | (任意) ブリッジグループ番号。指定できる範囲は 1 ~ 255 です。   |
| <b>active</b> [ <b>detail</b> ]  | (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)。   |
| <b>backbonefast</b>  | (任意) スパニングツリー BackboneFast ステータスを表示します。  |
| <b>blockedports</b>  | (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)。   |
| <b>bridge</b> [ <b>address</b>   <b>detail</b>   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>priority</b> [ <b>system-id</b> ]   <b>protocol</b> ]                                     | (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 (特権 EXEC モードの場合だけ使用可能なオプション キーワード)。   |
| <b>detail</b> [ <b>active</b> ]  | (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 ( <b>active</b> キーワードは特権 EXEC モードの場合だけ使用可能)。  |
| <b>inconsistentports</b>   | (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)。  |
| <b>interface</b> <i>interface-id</i> [ <b>active</b> [ <b>detail</b> ]   <b>cost</b>   <b>detail</b> [ <b>active</b> ]   <b>inconsistency</b>   <b>portfast</b>   <b>priority</b>   <b>rootcost</b>   <b>state</b> ] | (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 ( <b>portfast</b> および <b>state</b> 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としては、物理ポート、VLAN、ポート チャネルなどがあります。指定できる VLAN 範囲は 1 ~ 4094 です。指定できるポート チャネル範囲は 1 ~ 6 です。 |

|   |  |
|---|--|
| <b>mst</b> [ <b>configuration</b>   <b>digest</b> ]] [ <i>instance-id</i>   <b>detail</b>   <b>interface</b>   <i>interface-id</i> [ <b>detail</b> ]]                                   | <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"> <li>• <b>digest</b> : (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)。</li> </ul> <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"> <li>• <i>instance-id</i> : 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 を指定します。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。</li> <li>• <b>interface</b> <i>interface-id</i> : (任意) 物理ポート、VLAN、およびポートチャネルを含む、有効なインターフェイスを指定します。指定できる VLAN 範囲は 1 ~ 4094 です。ポートチャネルの範囲は 1 ~ 6 です。</li> <li>• <b>detail</b> : (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。</li> </ul> |
| <b>pathcost method</b>  | (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)。  |
| <b>root</b> [ <b>address</b>   <b>cost</b>   <b>detail</b>   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>port</b>   <b>priority</b>   <b>system-id</b> ]] | (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)。   |
| <b>summary</b> [ <b>totals</b> ]  | (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。 <i>IEEE Standard</i> という語は、スイッチ上で実行されている MST バージョンを識別します。   |

|   |  |
|---|--|
| <b>uplinkfast</b>   | (任意) スパニングツリー UplinkFast ステータスを表示します。  |
| <b>vlan</b> <i>vlan-id</i> [ <b>active</b>   <b>detail</b> ]   <b>backbonefast</b>   <b>blockedports</b>   <b>bridge</b>   <b>address</b>   <b>detail</b>   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>priority</b>   <b>system-id</b> ]   <b>protocol</b> ] | (任意) 特定の VLAN (特権 EXEC モードでのみ使用可能なキーワード) のスパニングツリー情報を表示します。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。 |

デフォルト なし

コマンドモード EXEC

#### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

#### 使用上のガイドライン

*vlan-id* 変数を省略した場合は、すべての VLAN のスパニングツリー インスタンスにコマンドが適用されます。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

#### 例

次の例では、**show spanning-tree active** コマンドの出力を示します。

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
            Address    0001.42e2.cdd0
            Cost      3038
            Port      24 (GigabitEthernet1/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49153 (priority 49152 sys-id-ext 1)
            Address    0003.fd63.9580
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 300
  Uplinkfast enabled

Interface          Role Sts Cost      Prio.Nbr Type
-----
Gi1/1              Root FWD 3019     128.24  P2p
<output truncated>
```

次の例では、**show spanning-tree detail** コマンドの出力を示します。

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 1 (GigabitEthernet1/1), cost of root path is 3038
```

## show spanning-tree

```

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 (GigabitEthernet1/1) 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 gigabitethernet1/1
Vlan          Role Sts Cost      Prio.Nbr Type
-----
VLAN0001      Root FWD 3019      128.24  P2p

```

```

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is enabled
BackboneFast is enabled
Pathcost method used is short

```

| Name     | Blocking | Listening | Learning | Forwarding | STP Active |
|----------|----------|-----------|----------|------------|------------|
| VLAN0001 | 1        | 0         | 0        | 11         | 12         |
| VLAN0002 | 3        | 0         | 0        | 1          | 4          |
| VLAN0004 | 3        | 0         | 0        | 1          | 4          |
| VLAN0006 | 3        | 0         | 0        | 1          | 4          |
| VLAN0031 | 3        | 0         | 0        | 1          | 4          |
| VLAN0032 | 3        | 0         | 0        | 1          | 4          |

<output truncated>

```

-----
37 vlans          109      0      0      47      156
Station update rate set to 150 packets/sec.

```

UplinkFast statistics

```

-----
Number of transitions via uplinkFast (all VLANs) : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0

```

BackboneFast statistics

```

-----
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs) : 0
Number of RLQ request PDUs received (all VLANs) : 0
Number of RLQ response PDUs received (all VLANs) : 0
Number of RLQ request PDUs sent (all VLANs) : 0
Number of RLQ response PDUs sent (all VLANs) : 0

```

次の例では、**show spanning-tree mst configuration** コマンドの出力を示します。

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0         1-9,21-4094
1         10-20
-----
```

次の例では、**show spanning-tree mst interface interface-id** コマンドの出力を示します。

```
Switch# show spanning-tree mst interface gigabitethernet1/1
GigabitEthernet1/1 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
port Gi1/1 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
-----
GigabitEthernet1/1 root FWD 200000 128 P2P bound(STP)
GigabitEthernet1/2 desg FWD 200000 128 P2P bound(STP)
Port-channel1 desg FWD 200000 128 P2P bound(STP)
```

## 関連コマンド

| コマンド   | 説明  |
|--|---|
| <a href="#">clear spanning-tree counters</a>           | スパニングツリーのカウンタをクリアします。   |
| <a href="#">clear spanning-tree detected-protocols</a> | プロトコル移行プロセスを再開します。  |
| <a href="#">spanning-tree backbonefast</a>             | BackboneFast 機能をイネーブルにします。  |
| <a href="#">spanning-tree bpduguard</a>                | インターフェイスでのブリッジプロトコル データ ユニット (BPDU) の送受信を禁止します。                   |
| <a href="#">spanning-tree bpduguard</a>                | BPDU を受信したインターフェイスを、errdisable ステートにします。                          |
| <a href="#">spanning-tree cost</a>                     | 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。                                     |
| <a href="#">spanning-tree extend system-id</a>         | 拡張システム ID 機能をイネーブルにします。   |
| <a href="#">spanning-tree guard</a>                    | 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。 |

| コマンド   | 説明   |
|--|--|
| <b>spanning-tree link-type</b>                       | 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。  |
| <b>spanning-tree loopguard default</b>               | 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。   |
| <b>spanning-tree mst configuration</b>               | 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。  |
| <b>spanning-tree mst cost</b>                        | MST の計算に使用するパス コストを設定します。  |
| <b>spanning-tree mst forward-time</b>                | 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。   |
| <b>spanning-tree mst hello-time</b>                  | 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。  |
| <b>spanning-tree mst max-age</b>                     | 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。   |
| <b>spanning-tree mst max-hops</b>                    | 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。   |
| <b>spanning-tree mst port-priority</b>               | インターフェイス プライオリティを設定します。  |
| <b>spanning-tree mst priority</b>                    | 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。  |
| <b>spanning-tree mst root</b>                        | 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。  |
| <b>spanning-tree port-priority</b>                   | インターフェイス プライオリティを設定します。  |
| <b>spanning-tree portfast (グローバル コンフィギュレーション)</b>    | 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。 |
| <b>spanning-tree portfast (インターフェイス コンフィギュレーション)</b> | 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。  |
| <b>spanning-tree uplinkfast</b>                      | リンクまたはスイッチに障害がある場合、またはスパニングツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択できるようにします。   |
| <b>spanning-tree vlan</b>                            | 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、EXEC モードで **show storm-control** をコマンド使用します。

**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]

| 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)。 |
| <b>broadcast</b>    | (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。              |
| <b>multicast</b>    | (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。               |
| <b>unicast</b>      | (任意) ユニキャスト ストームしきい値設定を表示します。                |

デフォルト なし

コマンドモード EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが導入されました。 |

**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
Interface      Filter State  Upper      Lower      Current
-----
Gi1/1         Forwarding   20 pps     10 pps     5 pps
Gi1/2         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 1/1
Interface  Filter State  Upper      Lower      Current
-----  -
Gig1/1     Forwarding  20 pps    10 pps     5 pps
```

表 2-31 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 2-31 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"> <li>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。</li> <li>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。</li> <li>Inactive : ストーム制御はディセーブルです。</li> </ul> |
| 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   |
|-------------------------------|--|
| <a href="#">storm-control</a> | 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単位 (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、特権 EXEC モードで **show system mtu** コマンドを使用します。

**show system mtu**

## 構文の説明

このコマンドにはキーワードまたは引数はありません。

## デフォルト

なし

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**system mtu** または **system mtu jumbo** グローバル コンフィギュレーション コマンドを使用して MTU の設定を変更した場合、スイッチをリセットしない限り、新しい設定は有効になりません。

システム MTU は 10/100 Mbps で動作するポートを、システム ジャンボ MTU はギガビット ポートを参照します。システム ルーティング MTU はルーテッドポートを参照します。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show system mtu** コマンドの出力を示します。

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1550 bytes
Routing MTU size is 1500 bytes.
```

## 関連コマンド

| コマンド                       | 説明   |
|----------------------------|--|
| <a href="#">system mtu</a> | ファストイーサネットポート、ギガビットイーサネットポート、またはルーテッドポートの MTU サイズを設定します。 |

# show udld

すべてのポートまたは指定されたポートの単方向リンク検出 (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、EXEC モードで **show udld** コマンドを使用します。

**show udld** [*interface-id*]

## 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。 |
|---------------------|---|

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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 2-32 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 gigabitethernet1/1
Interface gil/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: Gil/1
  Neighbor echo 1 device: Switch-B
  Neighbor echo 1 port: Gil/2
  Message interval: 5
  CDP Device name: Switch-A
```

表 2-32 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、 <b>unknown</b> 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、 <b>bidirectional</b> 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 マシンはアダプタイズ フェーズです。  |
| Message interval                                 | ローカル デバイスからアダプタイズ 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装置の両方で 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                                      | 装置名またはネイバーのシステム シリアル番号。装置名が設定されていないか、またはデフォルト ( <b>Switch</b> ) 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のデバイス名。  |
| 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                                 | ネイバーがアダプタイズ メッセージを送信する速度 (秒)。   |
| CDP device name                                  | CDP デバイス名またはシステム シリアル番号。装置名が設定されていないか、またはデフォルト ( <b>Switch</b> ) 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  |
|--------|-------------------|---|
|        | <b>uddl</b>       | 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。                                    |
|        | <b>uddl port</b>  | 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 <b>uddl</b> 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。 |
|        | <b>uddl reset</b> | 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、EXEC モードで **show version** コマンドを使用します。

## show version

### 構文の説明

このコマンドにはキーワードまたは引数はありません。

### デフォルト

なし

### コマンド モード

EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

### 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



(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。

次の例では、**show version** コマンドの出力を示します。

```
switch# show version
Cisco IOS Software, IES Software (IES-LANBASE-M), Version 15.0(1)EY, RELEASE SOFTWARE
(fc2) Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 19-May-08 12:47 by weiliu
Image text-base: 0x00003000, data-base: 0x01400000

ROM: Bootstrap program is IE 2000 boot loader
BOOTLDR: IES Boot Loader (IES-HBOOT-M), Version 15.0 [mchou-v122ldr0328 102]

Switch uptime is 2 days, 1 hour, 36 minutes System returned to ROM by power-on System
image file is ''flash:/ies-lanbase-mz.122-44.EX/ies-lanbase-mz.122-44.EX.bin''

cisco IE-3000-4TC (PowerPC405) processor with 126976K/4088K bytes of memory.
Processor board ID FHK1152UZRW
Last reset from power-on
1 Virtual Ethernet interface
20 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:1E:13:00:2D:00
Motherboard assembly number     : 73-10855-07
```

## ■ show version

```
Motherboard serial number      : FOC115040S9
Motherboard revision number    : 04
Model number                   : IE-3000-4TC
System serial number           : FHK1152UZRW
Top Assembly Part Number       : 800-28491-01
Hardware Board Revision Number : 0x02
CIP Serial Number              : 0x43313135
SKU Brand Name                 : Cisco

Switch Ports Model              SW Version      SW Image
-----
*    1 22    IE-3000-4TC    15.0(1)EY      IES-LANBASE-M

Configuration register is 0xF
```

# show vlan

スイッチ上のすべての設定済み VLAN または 1 つの VLAN の VLAN (VLAN ID または名前を指定した場合) を表示するには、EXEC モードで **show vlan** コマンドを使用します。

**show vlan [brief | id vlan-id | internal usage | mtu | name vlan-name | remote-span | summary]**

## 構文の説明

|                       |  |
|-----------------------|--|
| <b>brief</b>          | (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。  |
| <b>id vlan-id</b>     | (任意) VLAN ID 番号で特定された 1 つの VLAN に関する情報を表示します。vlan-id に指定できる範囲は 1 ~ 4094 です。  |
| <b>internal usage</b> | (任意) スイッチが内部的に使用する VLAN のリストを表示します。これらの VLAN は常に拡張範囲 (VLAN ID が 1006 ~ 4094) 内のものです。これらの VLAN を内部使用から削除しないと、vlan グローバル コンフィギュレーション コマンドを使用して、これらの IDS で VLAN を作成できません。 |
| <b>mtu</b>            | (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単位 (MTU) サイズを表示します。  |
| <b>name vlan-name</b> | (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。   |
| <b>remote-span</b>    | (任意) Remote SPAN (RSPAN) VLAN に関する情報を表示します。  |
| <b>summary</b>        | (任意) VLAN サマリー情報を表示します。  |



(注) **ifindex** キーワードは、コマンドラインのヘルプストリングには表示されていますが、サポートされていません。

## デフォルト

なし

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**show vlan mtu** コマンド出力では、MTU\_Mismatch 列に VLAN 内のすべてのポートに同じ MTU があるかどうかを示します。この列に **yes** が表示されている場合、VLAN の各ポートに別々の MTU があり、パケットが、大きい MTU を持つポートから小さい MTU を持つポートにスイッチングされると、ドロップされることがあります。VLAN に SVI がない場合、ハイフン (-) 記号が SVI\_MTU 列に表示されます。MTU-Mismatch 列に **yes** が表示されている場合、MiniMTU を持つポートと MaxMTU を持つポート名が表示されます。

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 2-33 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show vlan
VLAN Name                Status    Ports
-----
1    default                active   Fa1/1, Fa1/2, Fa1/3, Fa1/4
                                   Fa2/1, Fa2/2, Fa2/3, Fa2/4
                                   Fa2/5, Fa2/6, Fa2/7, Fa2/8
                                   Fa3/1, Fa3/2, Fa3/3, Fa3/4
                                   Fa3/5, Fa3/6, Fa3/7, Fa3/8
                                   Gi1/1, Gi1/2
2    Tes                    active   Fa1/3, Fa2/5, Fa2/6
1002 fddi-default          act/unsup
1003 token-ring-default   act/unsup
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
2    enet    100002   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

Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----
20     25     isolated Fa1/13, Fa1/20, Fa1/22, Gi1/1,
20     30     community Fa1/1, Fa1/20, Fa1/21, Gi1/1,

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
                                   Fa0/24, Gi0/1, Gi0/2

<output truncated>

2    VLAN0002                active
3    VLAN0003                active

<output truncated>

1000 VLAN1000              active
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default        active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet    100001   1500   -     -     -     -     -     1002 1003
2    enet    100002   1500   -     -     -     -     -     0     0
```

```

3   enet  100003   1500 - - - - - 0 0
<output truncated>

1005 trnet 101005   1500 - - - - - ibm - 0 0

Remote SPAN VLANs
-----
Primary Secondary Type          Ports
-----
Primary Secondary Type Ports
-----
20      25      isolated 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
<output truncated>

```

表 2-33 show vlan コマンドの出カフィールド

| 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 の最大伝送単位サイズ。  |
| Parent            | 親 VLAN (存在する場合)。  |
| RingNo            | VLAN のリング番号 (該当する場合)。   |
| BrdgNo            | VLAN のブリッジ番号 (該当する場合)。  |
| Stp               | VLAN で使用されるスパニングツリー プロトコル タイプ。  |
| BrdgMode          | この VLAN のブリッジング モード: 可能な値はソースルートブリッジング (SRB) およびソースルート トランスペアレント (SRT) で、デフォルトは SRB です。 |
| Trans1            | トランスレーションブリッジ 1。  |
| Trans2            | トランスレーションブリッジ 2。  |
| Remote SPAN VLANs | 設定されている RSPAN VLAN を識別します。  |

次の例では、**show vlan summary** コマンドの出力を示します。

```

Switch> show vlan summary
Number of existing VLANs      : 45
Number of existing VTP VLANs  : 45
Number of existing extended VLANs : 0

```

次の例では、**show vlan id** コマンドの出力を示します。

```

Switch# show vlan id 2
VLAN Name          Status  Ports
-----

```

## show vlan

```

2    VLAN0200                                active Fa1/3, Fa2/5, Fa2/6

2    VLAN0200                                active    Fa1/3, Fa2/5, Fa2/6
VLAN Type SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
2    enet  100002    1500   -      -      -      -      -      0      0

Remote SPAN VLAN
-----
Disabled

```

次の例では、**show vlan internal usage** コマンドの出力を示します。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 FastEthernet1/23
1026 FastEthernet1/24

```

## 関連コマンド

| コマンド                            | 説明   |
|---------------------------------|--|
| <a href="#">switchport mode</a> | ポートの VLAN メンバーシップ モードを設定します。                           |
| <a href="#">vlan</a>            | 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、特権 EXEC モードで **show vlan access-map** コマンドを使用します。

**show vlan access-map** [*mapname*]



(注)

このコマンドは、スイッチが IP サービス イメージを稼働している場合にだけ使用できます。

## 構文の説明

*mapname* (任意) 特定の VLAN アクセス マップ名。

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## 例

次の例では、**show vlan access-map** コマンドの出力を示します。

```
Switch# show vlan access-map
Vlan access-map "SecWiz" 10
  Match clauses:
    ip address: SecWiz_Gi0_3_in_ip
    ip address: SecWiz_Fal0_3_in_ip

  Action:
    forward
```

## 関連コマンド

| コマンド                             | 説明  |
|----------------------------------|---|
| <a href="#">show vlan filter</a> | 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。 |
| <a href="#">vlan access-map</a>  | 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。                       |
| <a href="#">vlan filter</a>      | 1 つ以上の VLAN に、VLAN マップを適用します。                                 |

# show vlan filter

すべての VLAN フィルタまたは特定の 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、特権 EXEC モードで **show vlan filter** コマンドを使用します。

**show vlan filter** [*access-map name* | *vlan vlan-id*]



(注)

このコマンドは、スイッチが IP サービス イメージを稼働している場合にだけ使用できます。

## 構文の説明

|                        |  |
|------------------------|--|
| <b>access-map name</b> | (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。              |
| <b>vlan vlan-id</b>    | (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。 |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 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  |
|--------------------------------------|---|
| <a href="#">show vlan access-map</a> | 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。 |
| <a href="#">vlan access-map</a>      | 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。             |
| <a href="#">vlan filter</a>          | 1 つ以上の VLAN に、VLAN マップを適用します。                       |

# show vmps

VLAN Query Protocol (VQP) バージョン、再確認間隔、再試行回数、VLAN メンバーシップ ポリシー サーバ (VMPS) IP アドレス、および現在のサーバとプライマリ サーバを表示するか、または **statistics** キーワードを使用してクライアント側の統計情報を表示するには、特権 EXEC モードで **show vmps** コマンドを使用します。

**show vmps [statistics]**

|          |                   |                                     |
|----------|-------------------|-------------------------------------|
| 構文の説明    | <b>statistics</b> | (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。 |
| デフォルト    | なし                |                                     |
| コマンド モード | EXEC              |                                     |
| コマンド履歴   | <b>リリース</b>       | <b>変更内容</b>                         |
|          | 15.0(1)EY         | このコマンドが導入されました。                     |

**使用上のガイドライン** 文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

**例** 次の例では、**show vmps** コマンドの出力を示します。

```
Switch> show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          other
```

次の例では、**show vmps statistics** コマンドの出力を示します。表 2-34 に、表示される各フィールドの説明を示します。

```
Switch> show vmps statistics
VMPS Client Statistics
-----
VQP Queries:          0
VQP Responses:        0
VMPS Changes:         0
VQP Shutdowns:       0
VQP Denied:           0
VQP Wrong Domain:     0
VQP Wrong Version:    0
VQP Insufficient Resource: 0
```

表 2-34 show vmps statistics のフィールドの説明

| フィールド                     | 説明  |
|---------------------------|---|
| VQP Queries               | クライアントから VMPS に送信されるクエリー数。  |
| VQP Responses             | VMPS からクライアントに送信される応答数。   |
| VMPS Changes              | サーバ間で VMPS を変更した回数。   |
| VQP Shutdowns             | ポートをシャットダウンするために VMPS が応答を送信した回数。クライアントはポートをディセーブルにし、このポート上のすべてのダイナミックアドレスをアドレス テーブルから削除します。接続を復元するには、管理上ポートを再びイネーブル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 VTP 管理ドメインが設定されていないことを意味します。   |
| VQP Wrong Version         | クエリー パケットのバージョン フィールドに、VMPS でサポートされているバージョンよりも大きい値が格納される回数。ポートの VLAN 割り当ては変更されません。スイッチは VMPS バージョン 1 要求だけを送信します。  |
| VQP Insufficient Resource | リソースの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  |
|---------------------------------|---|
| <b>clear vmps statistics</b>    | 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。                    |
| <b>vmps reconfirm (特権 EXEC)</b> | 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。 |
| <b>vmps retry</b>               | 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。                     |
| <b>vmps server</b>              | プライマリ VMPS、および最大で 3 台のセカンダリ サーバを設定します。            |

# show vtp

VLAN トランッキング プロトコル (VTP) 管理ドメイン、ステータス、およびカウンタに関する一般情報を表示するには、EXEC モードで **show vtp** コマンドを使用します。

```
show vtp {counters | devices [conflicts] | interface [interface-id] | password | status}
```

## 構文の説明

|                                 |  |
|---------------------------------|--|
| <b>counters</b>                 | スイッチの VTP 統計情報を表示します。  |
| <b>password</b>                 | 設定された VTP パスワードを表示します。   |
| <b>devices</b>                  | ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。このキーワードは、スイッチが VTP バージョン 3 を実行していない場合だけ適用されます。                       |
| <b>conflicts</b>                | (任意) 競合するプライマリ サーバを持つ VTP バージョン 3 デバイスに関する情報を表示します。スイッチが VTP トランスペアレント モードまたは VTP オフ モードにある場合、このコマンドは無視されます。 |
| <b>interface</b> [interface-id] | すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。interface-id には物理インターフェイスまたはポート チャネルを指定できます。          |
| <b>status</b>                   | VTP 管理ドメインのステータスに関する一般情報を表示します。  |

## デフォルト

なし

## コマンド モード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

スイッチが VTP バージョン 3 を実行中に **show vtp password** コマンドを入力すると、表示は次のルールに従います。

- **password password** グローバル コンフィギュレーション コマンドで **hidden** キーワードを指定せず、スイッチ上で暗号化がイネーブルでない場合、パスワードはクリア テキストで表示されます。
- **password password** コマンドで **hidden** キーワードを指定せず、スイッチ上で暗号化がイネーブルの場合、暗号化されたパスワードが表示されます。
- **password password** コマンドに **hidden** キーワードが含まれていた場合、16 進数の秘密キーが表示されます。

文字列では、大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

## show vtp

## 例

次の例では、**show vtp devices** コマンドの出力を示します。**Conflict** 列の **Yes** は、応答するサーバがその機能のローカル サーバと競合していることを意味します。つまり、同じドメイン内の 2 つのスイッチは、データベースに対して同じプライマリ サーバを持ちません。

```
Switch# show vtp devices

Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf switch ID      Primary Server Revision  System Name
-----
VLAN          Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST           No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN          Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

次の例では、**show vtp counters** コマンドの出力を示します。表 2-35 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show vtp counters

VTP statistics:
Summary advertisements received      : 0
Subset advertisements received      : 0
Request advertisements received     : 0
Summary advertisements transmitted  : 6970
Subset advertisements transmitted    : 0
Request advertisements transmitted  : 0
Number of config revision errors    : 0
Number of config digest errors      : 0
Number of V1 summary errors         : 0

VTP pruning statistics:

Trunk          Join Transmitted Join Received  Summary advts received from
-----
Fa1/7          0                0                0
Fa1/8          0                0                0
Gi1/1          0                0                0
Gi1/2          0                0                0
```

表 2-35 show vtp counters のフィールドの説明

| フィールド                              | 説明   |
|------------------------------------|--|
| Summary advertisements received    | トランク ポート上でこのスイッチが受信するサマリー アドバタイズの数。サマリー アドバタイズには、管理ドメイン名、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。 |
| Subset advertisements received     | トランク ポート上でこのスイッチが受信するサブセット アドバタイズの数。サブセット アドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。  |
| Request advertisements received    | トランク ポート上でこのスイッチが受信するアドバタイズ要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。                                |
| Summary advertisements transmitted | トランク ポート上でこのスイッチが送信するサマリー アドバタイズの数。サマリー アドバタイズには、管理ドメイン名、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。 |
| Subset advertisements transmitted  | トランク ポート上でこのスイッチが送信するサブセット アドバタイズの数。サブセット アドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。  |

表 2-35 show vtp counters のフィールドの説明 (続き)

| フィールド  | 説明  |
|--|---|
| Request advertisements transmitted                     | トランク ポート上でこのスイッチが送信するアドバタイズ要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。   |
| Number of configuration revision errors                | リビジョン エラーの数。<br>新しい VLAN の定義、既存 VLAN の削除、中断、または再開、あるいは既存 VLAN のパラメータ変更を行うと、スイッチのコンフィギュレーション リビジョン番号が増加します。<br>リビジョン番号がスイッチのリビジョン番号と一致するにもかかわらず、MD5 ダイジェスト値が一致しないアドバタイズをスイッチが受信すると、リビジョン エラーが増加します。このエラーは、2つのスイッチの VTP パスワードが異なるか、またはスイッチの設定が異なることを意味します。<br>これらのエラーが発生した場合、スイッチは着信アドバタイズのフィルタリング中であり、ネットワーク内で VTP データベースが同期しなくなります。 |
| Number of configuration digest errors                  | MD5 ダイジェスト エラーの数。<br>サマリー パケット内の MD5 ダイジェストと、計算された受信済みアドバタイズの MD5 ダイジェストが一致しない場合は、ダイジェスト エラーが増加します。このエラーは、通常、2つのスイッチの VTP パスワードが異なることを意味します。この問題を解決するには、すべてのスイッチで VTP パスワードが同じになるようにします。<br>これらのエラーが発生した場合、スイッチは着信アドバタイズのフィルタリング中であり、ネットワーク内で VTP データベースが同期しなくなります。   |
| Number of V1 summary errors                            | バージョン 1 エラーの数。<br>VTP V2 モードのスイッチが VTP バージョン 1 フレームを受信すると、バージョン 1 サマリー エラーが増加します。これらのエラーは、少なくとも1つのネイバースイッチ上で VTP バージョン 1 が稼働しているか、または V2 モードがディセーブルの状態でも VTP バージョン 2 が稼働していることを意味します。この問題を解決するには、VTP V2 モードのスイッチの設定をディセーブルに変更します。   |
| Join Transmitted                                       | トランク上で送信された VTP プルーニング メッセージの数。   |
| Join Received  | トランク上で受信された VTP プルーニング メッセージの数。   |
| Summary Advts Received from non-pruning-capable device | トランク上で受信された、プルーニングをサポートしていないデバイスからの VTP サマリー メッセージの数。   |

次の例では、VTP バージョン 2 を実行するスイッチに対する **show vtp status** コマンドの出力を示します。表 2-36 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 45
VTP Operating Mode         : Transparent
VTP Domain Name            : shared_testbed1
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Enabled
MD5 digest                  : 0x3A 0x29 0x86 0x39 0xB4 0x5D 0x58 0xD7
```

## ■ show vtp

表 2-36 show vtp status のフィールドの説明

| フィールド                           | 説明   |
|---------------------------------|--|
| VTP Version                     | スイッチ上で動作している VTP バージョンを表示します。デフォルトでは、スイッチはバージョン 1 を実行しますが、バージョン 2 に設定することもできます。  |
| Configuration Revision          | このスイッチの現在のコンフィギュレーション リビジョン番号。   |
| Maximum VLANs Supported Locally | ローカルにサポートされている VLAN の最大数。  |
| Number of Existing VLANs        | 既存の VLAN 数。  |
| VTP Operating Mode              | <p>VTP 動作モード（サーバ、クライアント、またはトランスペアレント）を表示します。</p> <p><b>Server :</b> VTP サーバ モードのスイッチは VTP に対してイネーブルにされています。また、このスイッチはアドバタイズメントを送信します。スイッチで VLAN を設定できます。このスイッチを使用すると、起動後に、現在の VTP データベース内のすべての VLAN 情報を、NVRAM から復元できます。デフォルトでは、すべてのスイッチが VTP サーバです。</p> <p><b>(注)</b> スイッチが設定を NVRAM に書き込んでいる間に障害を検出し、NVRAM が機能するまでサーバモードに戻ることができない場合、スイッチは VTP サーバモードから VTP クライアントモードに自動的に変わります。</p> <p><b>Client :</b> VTP クライアントモードのスイッチは VTP に対してイネーブルにされています。また、このスイッチはアドバタイズメントを送信しますが、VLAN コンフィギュレーションを保存するには不揮発性ストレージが足りません。スイッチでは VLAN を設定できません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。</p> <p><b>Transparent :</b> VTP トランスペアレントモードのスイッチは VTP に対してディセーブルにされています。アドバタイズメントの送信や、他のデバイスにより送信されたアドバタイズメントからの学習は行われません。また、ネットワーク内の他のデバイスの VLAN コンフィギュレーションには影響を与えません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。</p> |
| VTP Domain Name                 | スイッチの管理ドメインを特定する名前。  |
| VTP Pruning Mode                | プルニングがイネーブルかまたはディセーブルかを表示します。VTP サーバでプルニングをイネーブルにすると、管理ドメイン全体でプルニングが有効になります。プルニングを使用すると、トラフィックが適切なネットワーク デバイスにアクセスするために使用しなければならないトランク リンクへのフラッドングトラフィックが制限されます。   |
| VTP V2 Mode                     | VTP バージョン 2 モードがイネーブルかどうかを表示します。すべての VTP バージョン 2 スイッチは、デフォルトでバージョン 1 モードで動作します。各 VTP スイッチは他のすべての VTP デバイスの機能を自動的に検出します。VTP デバイス ネットワーク内のすべての VTP スイッチがバージョン 2 モードで動作可能な場合だけ、ネットワークをバージョン 2 に設定してください。  |
| VTP Traps Generation            | VTP トラップをネットワーク管理ステーションに送信するかどうかを表示します。  |
| MD5 Digest                      | VTP 設定の 16 バイトチェックサム。  |
| Configuration Last Modified     | 最後に行った設定変更の日付と時刻を表示します。データベースの設定変更の原因となったスイッチの IP アドレスを表示します。  |

次の例では、VTP バージョン 3 が稼働しているスイッチに対する **show vtp status** コマンドの出力を示します。

```
Switch> show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 3
VTP Domain Name         : Cisco
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 0021.1bcd.c700

Feature VLAN:
-----
VTP Operating Mode      : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID              : 0000.0000.0000
Primary Description    :
MD5 digest              : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                       : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
-----
VTP Operating Mode      : Client
Configuration Revision : 0
Primary ID              : 0000.0000.0000
Primary Description    :
MD5 digest              : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                       : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
-----
VTP Operating Mode      : Transparent
```

#### 関連コマンド

| コマンド                           | 説明                                       |
|--------------------------------|--|
| <b>clear vtp counters</b>      | VTP およびプルーニング カウンタをクリアします。               |
| <b>vtp (グローバル コンフィギュレーション)</b> | VTP のファイル名、インターフェイス名、ドメイン名、およびモードを設定します。 |

# shutdown

インターフェイスをディセーブルにします。ディセーブルになったインターフェイスを再開するには、このコマンドの **no** 形式を使用し、**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。

**shutdown**

**no shutdown**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

ポートはイネーブルです (シャットダウンしません)。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**shutdown** コマンドを入力すると、ポートは転送を停止します。ポートをイネーブルにするには、**no shutdown** コマンドを使用します。

削除、中断、またはシャットダウンされた VLAN に割り当てられているスタティック アクセス ポートに **no shutdown** コマンドを使用しても、無効です。ポートを再びイネーブルにするには、まずポートをアクティブ VLAN のメンバにする必要があります。

**shutdown** コマンドは指定のインターフェイス上のすべての機能をディセーブルにします。

また、このコマンドはインターフェイスが使用不可であることをマーク付けします。インターフェイスがディセーブルかどうかを確認するには、**show interfaces** 特権 EXEC コマンドを使用します。シャットダウンされたインターフェイスは、管理上のダウンとして画面に表示されます。

## 例

次に、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例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# shutdown
```

```
Switch(config)# interface gigabitethernet1/2
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  |
|---------------------------------|---|
| <a href="#">show interfaces</a> | 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

指定した VLAN でローカルトラフィックをシャットダウン（一時停止）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、**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。

**shutdown vlan** *vlan-id*

**no shutdown vlan** *vlan-id*

|                   |   |  |
|-------------------|---|--|
| <b>構文の説明</b>      | <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。VLAN トランッキングプロトコル (VTP) 環境のデフォルト VLAN として定義された VLAN、および拡張範囲 VLAN (ID が 1005 を超える VLAN) は、シャットダウンできません。デフォルトの VLAN は 1 および 1002 ~ 1005 です。 |
| <b>デフォルト</b>      | なし  |  |
| <b>コマンドモード</b>    |   | グローバル コンフィギュレーション  |
| <b>コマンド履歴</b>     | <b>リリース</b>   | <b>変更箇所</b>  |
|                   | 15.0(1)EY   | このコマンドが追加されました。  |
| <b>使用上のガイドライン</b> | <b>shutdown vlan</b> コマンドは、VTP データベース内の VLAN 情報を変更しません。このコマンドはローカルトラフィックをシャットダウンしますが、スイッチは VTP 情報をアドバタイズし続けます。                          |  |
| <b>例</b>          | 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。<br>Switch(config)# <b>shutdown vlan 2</b><br><br>設定を確認するには、 <b>show vlan</b> 特権 EXEC コマンドを入力します。 |  |
| <b>関連コマンド</b>     | <b>コマンド</b>   | <b>説明</b>  |
|                   | <b>shutdown</b><br>(config-vlan モード)  | config-vlan モード ( <b>vlan vlan-id</b> 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。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。                 |

# small-frame violation rate

指定されたレートで小さいフレーム（67 バイト以下）の VLAN タグ付きパケットを受信した場合にインターフェイスが `errdisable` になるレート（しきい値）を設定するには、**small-frame violation rate** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの `no` 形式を使用します。

**small-frame violation rate** *pps*

**no small-frame violation rate** *pps*

## 構文の説明

*pps* 小さいフレームを受信するインターフェイスが `errdisable` となるしきい値を指定します。指定できる範囲は、1 ~ 10,000 pps（パケット/秒）です。

## デフォルト

この機能はディセーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、ポートが小さいフレームを受信すると `errdisable` となる伝送速度（しきい値）をイネーブルにします。67 フレーム以下のパケットが小さいフレームと見なされます。

各ポートで小さいフレームと見なすしきい値をグローバルにイネーブルにするには、**errdisable detect cause small-frame** グローバル コンフィギュレーション コマンドを使用します。

ポートが自動的に再びイネーブルになるように設定するには、**errdisable recovery cause small-frame** グローバル コンフィギュレーション コマンドを使用します。回復時間を設定するには、**errdisable recovery interval interval** グローバル コンフィギュレーション コマンドを使用します。

## 例

次の例では、小さい着信フレームが 10,000 pps で到達した場合にポートが `errdisable` となるようにする小さいフレームの着信速度の機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# small-frame violation rate 10000
```

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

## 関連コマンド

| コマンド                                       | 説明   |
|--|--|
| <b>errdisable detect cause small-frame</b> | 着信フレームが最小サイズより小さく、指定した伝送速度（しきい値）で到着したスイッチ ポートがあれば、そのポートを <code>errdisable</code> 状態にします。 |

| コマンド   | 説明                                |
|--|-----------------------------------|
| <code>errdisable recovery cause small-frame</code> | 回復タイマーをイネーブルにします。                 |
| <code>show interfaces</code>                       | 入出力フロー制御を含むスイッチのインターフェイス設定を表示します。 |

## snmp-server enable traps

スイッチでさまざまなトラップの簡易ネットワーク管理プロトコル (SNMP) 通知を送信したり、ネットワーク管理システム (NMS) に要求を通知したりできるようにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps [bgp | bridge [newroot] [topologychange] | cluster | config |
copy-config | cpu [threshold] | dot1x [auth-fail-vlan | guest-vlan | no-auth-fail-vlan |
no-guest-vlan] | entity | envmon [fan | shutdown | status | supply | temperature] | errdisable
[notification-rate value] | flash [insertion | removal] | hsrp | ipmulticast | mac-notification
[change] [move] [threshold] | ospf [cisco-specific | errors | lsa | rate-limit | retransmit |
state-change] | pim [invalid-pim-message | neighbor-change | rp-mapping-change] |
port-security [trap-rate value] | rtr | snmp [authentication | coldstart | linkdown | linkup |
warmstart] | storm-control trap-rate value | stpx [inconsistency] [root-inconsistency]
[loop-inconsistency] | syslog | tty | vlan-membership | vlancreate | vlandelete | vtp]
```

```
no snmp-server enable traps [bgp | bridge [newroot] [topologychange] | cluster | config |
copy-config | cpu [threshold] | dot1x [auth-fail-vlan | guest-vlan | no-auth-fail-vlan |
no-guest-vlan] | entity | envmon [fan | shutdown | status | supply | temperature] | errdisable
[notification-rate value] | flash [insertion | removal] | hsrp | ipmulticast | mac-notification
[change] [move] [threshold] | ospf [cisco-specific | errors | lsa | rate-limit | retransmit |
state-change] | pim [invalid-pim-message | neighbor-change | rp-mapping-change] |
port-security [trap-rate value] | rtr | snmp [authentication | coldstart | linkdown | linkup |
warmstart] | storm-control trap-rate value | stpx [inconsistency] [root-inconsistency]
[loop-inconsistency] | syslog | tty | vlan-membership | vlancreate | vlandelete | vtp]
```

### 構文の説明

|  |   |
|--|---|
| <b>bgp</b>                               | (任意) ボーダー ゲートウェイ プロトコル (BGP) ステート変更トラップをイネーブルにします。<br><br>(注) このキーワードは、スイッチに IP サービス 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。   |
| <b>bridge [newroot] [topologychange]</b> | (任意) STP ブリッジ MIB トラップを生成します。<br><br><ul style="list-style-type: none"> <li>• <b>newroot</b> : (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。</li> <li>• <b>topologychange</b> : (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。</li> </ul> |
| <b>cluster</b>                           | (任意) クラスタ トラップをイネーブルにします。   |
| <b>config</b>                            | (任意) SNMP 設定トラップをイネーブルにします。   |
| <b>config-ctid</b>                       | (任意) SNMP CTID トラップをイネーブルにします。  |
| <b>copy-config</b>                       | (任意) SNMP コピー設定トラップをイネーブルにします。  |
| <b>cpu</b>                               | (任意) 選択 CPU 関連トラップを許可します。任意の <b>threshold</b> キーワードは、しきい値違反トラップをイネーブルにします。  |

|  |   |
|--|---|
| <b>dot1x</b> [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。</p> <ul style="list-style-type: none"> <li>• <b>auth-fail-vlan</b> : (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。</li> <li>• <b>guest-vlan</b> : (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。</li> <li>• <b>no-auth-fail-vlan</b> : (任意) 制限 VLAN が設定されていないために、ポートが制限 VLAN を開始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。</li> <li>• <b>no-guest-vlan</b> : (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 を開始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。</li> </ul> <p>(注) キーワードを何も指定せずに <b>snmp-server enable traps dot1x</b> 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> |
| <b>entity</b>  | (任意) SNMP エンティティ トラップを送信します。  |
| <b>envmon</b> [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。</p> <ul style="list-style-type: none"> <li>• <b>fan</b> : (任意) ファン トラップをイネーブルにします。</li> <li>• <b>shutdown</b> : (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。</li> <li>• <b>status</b> : (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。</li> <li>• <b>supply</b> : (任意) 環境モニタ powersupply トラップをイネーブルにします。</li> <li>• <b>temperature</b> : (任意) 環境モニタ温度トラップをイネーブルにします。</li> </ul>  |
| <b>errdisable</b> [notification-rate value]                                    | (任意) errdisable トラップをイネーブルにします。notification-rate キーワードを使用して、分単位で送信される errdisable トラップの最大値を設定します。指定できる範囲は 0 ~ 10000 です。デフォルト値は 0 です (制限はなく、トラップは発生するたびに送信されます)。  |
| <b>flash</b>   | <p>(任意) SNMP フラッシュ通知をイネーブルにします。</p> <ul style="list-style-type: none"> <li>• <b>insertion</b> : (任意) フラッシュの挿入通知をイネーブルにします。</li> <li>• <b>removal</b> : (任意) フラッシュ削除通知をイネーブルにします。</li> </ul>   |
| <b>hsrp</b>  | (任意) ホットスタンバイ ルータ プロトコル (HSRP) トラップをイネーブルにします。  |
| <b>mac-notification</b>  | <p>(任意) MAC アドレス通知トラップをイネーブルにします。</p> <ul style="list-style-type: none"> <li>• <b>change</b> : MAC アドレス変更通知トラップをイネーブルにします。</li> <li>• <b>move</b> : MAC アドレス移動通知トラップをイネーブルにします。</li> <li>• <b>threshold</b> : MAC アドレス テーブルしきい値トラップイネーブルにします。</li> </ul>  |

|  |   |
|--|---|
| <b>ospf</b> [ <b>cisco-specific</b>   <b>errors</b>   <b>lsa</b>   <b>rate-limit</b>   <b>retransmit</b>   <b>state-change</b> ] | (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。 <ul style="list-style-type: none"> <li>• <b>cisco-specific</b> : (任意) シスコ固有のトラップをイネーブルにします。</li> <li>• <b>errors</b> : (任意) エラー トラップをイネーブルにします。</li> <li>• <b>lsa</b> : (任意) リンクステート アドバタイズメント (LSA) トラップをイネーブルにします。</li> <li>• <b>rate-limit</b> : (任意) レート制限トラップをイネーブルにします。</li> <li>• <b>retransmit</b> : (任意) パケット再送信トラップをイネーブルにします。</li> <li>• <b>state-change</b> : (任意) ステート変更トラップをイネーブルにします。</li> </ul> |
| <b>pim</b> [ <b>invalid-pim-message</b>   <b>neighbor-change</b>   <b>rp-mapping-change</b> ]                                    | (任意) プロトコル独立型マルチキャスト (PIM) トラップをイネーブルにします。 <ul style="list-style-type: none"> <li>• <b>invalid-pim-message</b> : (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。</li> <li>• <b>neighbor-change</b> : (任意) PIM ネイバー変更トラップをイネーブルにします。</li> <li>• <b>rp-mapping-change</b> : (任意) ランデブー ポイント (RP) マッピング変更トラップをイネーブルにします。</li> </ul>   |
| <b>port-security</b> [ <b>trap-rate</b> <i>value</i> ]   | (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、 <b>trap-rate</b> キーワードを使用します。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 です (制限はなく、トラップは発生するたびに送信されます)。   |
| <b>rtr</b>   | (任意) SNMP Response Time Reporter トラップをイネーブルにします。  |
| <b>snmp</b> [ <b>authentication</b>   <b>coldstart</b>   <b>linkdown</b>   <b>linkup</b>   <b>warmstart</b> ]                    | (任意) SNMP トラップをイネーブルにします。 <ul style="list-style-type: none"> <li>• <b>authentication</b> : (任意) 認証トラップをイネーブルにします。</li> <li>• <b>coldstart</b> : (任意) コールドスタート トラップをイネーブルにします。</li> <li>• <b>linkdown</b> : (任意) リンクダウン トラップをイネーブルにします。</li> <li>• <b>linkup</b> : (任意) リンクアップ トラップをイネーブルにします。</li> <li>• <b>warmstart</b> : (任意) ウォーム スタート トラップをイネーブルにします。</li> </ul>   |
| <b>storm-control</b> <b>trap-rate</b> <i>value</i>   | (任意) storm-control 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、 <b>trap-rate</b> キーワードを使用します。指定できる範囲は 0 ~ 1000 です。デフォルト値は 0 です (制限はなく、トラップは発生するたびに送信されます)。  |
| <b>stp</b> [ <b>inconsistency</b>   <b>root-inconsistency</b>   <b>loop-inconsistency</b> ]                                      | (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"> <li>• <b>inconsistency</b> : (任意) SNMP STPX MIB の矛盾更新トラップをイネーブルにします。</li> <li>• <b>root-inconsistency</b> : (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。</li> <li>• <b>loop-inconsistency</b> : (任意) SNMP STPX MIB ループ矛盾更新トラップをイネーブルにします。</li> </ul>   |
| <b>syslog</b>  | (任意) SNMP syslog トラップをイネーブルにします。  |
| <b>tty</b>   | (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。   |

|                        |  |
|------------------------|--|
| <b>vlan-membership</b> | (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。       |
| <b>vlancreate</b>      | (任意) SNMP VLAN 作成トラップをイネーブルにします。             |
| <b>vlandelete</b>      | (任意) SNMP VLAN 削除トラップをイネーブルにします。             |
| <b>vtp</b>             | (任意) VLAN トランキンング プロトコ (VTP) トラップをイネーブルにします。 |



(注) **insertion** および **removal** 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で使用します。

#### 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            |
|-----------|-----------------|
| 15.0(1)EY | 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、すべてのタイプが送信されます。

**snmp-server enable traps** コマンドは、トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにします。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

CPU しきい値通知のタイプおよび値を設定するには、**process cpu threshold type** グローバル コンフィギュレーション コマンドを使用します。

#### 例

次の例では、NMS に VTP トラップを送信する方法を示します。

```
Switch(config)# snmp-server enable traps vtp
```

## 関連コマンド

| コマンド                             | 説明   |
|----------------------------------|--|
| <code>show running-config</code> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <code>snmp-server host</code>    | SNMP トラップを受信するホストを指定します。   |

# snmp-server host

簡易ネットワーク管理プロトコル (SNMP) による通知の受信者 (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 [udp-port port | 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。  |
| <b>udp-port port</b>      | (任意) トラップを受信するホストのユーザ データグラム プロトコル (UDP) ポート番号を設定します。指定できる範囲は 0 ~ 65535 です。  |
| <b>informs   traps</b>    | (任意) このホストに SNMP トラップを送信または通知します。  |
| <b>version 1   2c   3</b> | (任意) トラップの送信に使用する SNMP のバージョンを指定します。<br>次のキーワードがサポートされています。<br><b>1</b> : SNMPv1。情報の場合は、このオプションを使用できません。<br><b>2c</b> : SNMPv2C。<br><b>3</b> : 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"> <li><b>auth</b> : (任意) Message Digest 5 (MD5) と Secure Hash Algorithm (SHA) パケット認証をイネーブルにします。</li> <li><b>noauth</b> (デフォルト) : noAuthNoPriv セキュリティ レベル。[<b>auth   noauth   priv</b>] 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。</li> <li><b>priv</b> (任意) : データ暗号規格 (DES) によるパケット暗号化 (<i>privacy</i> と呼びます) をイネーブルにします。</li> </ul> <b>(注)</b> <b>priv</b> 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。 |
| <b>vrf vrf-instance</b>   | (任意) バーチャル プライベート ネットワーク (VPN) ルーティング インスタンスとこのホストの名前を指定します。   |
| <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。 <b>snmp-server host</b> 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、 <b>snmp-server community</b> 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、 <b>snmp-server host</b> コマンドを使用することを推奨します。<br><b>(注)</b> 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。   |
| <i>notification-type</i>  | (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ものを含めることが可能です。 <b>alarms</b> 、 <b>auth-framework</b> 、 <b>bridge</b> 、および <b>cluster</b> 。CLI オンライン ヘルプを使用して、完全なリストを取得できます。   |

## デフォルト

このコマンドは、デフォルトでディセーブルです。通知は送信されません。

15.0(1)EY : キーワードを指定せずにこのコマンドを入力すると、デフォルトでは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            |
|-----------|-----------------|
| 15.0(1)EY | 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 ストリング `comaccess` を設定し、このストリングによる、アクセス リスト 10 を介した SNMP ポーリング アクセスを禁止します。

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

次の例では、名前 `myhost.cisco.com` で指定されたホストに SNMP トラップを送信する方法を示します。コミュニティ ストリングは、`comaccess` として定義されています。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティ ストリング `public` を使用して、すべてのトラップをホスト `myhost.cisco.com` に送信するようにスイッチをイネーブルにする方法を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

## 関連コマンド

| コマンド                                  | 説明   |
|---------------------------------------|--|
| <code>show running-config</code>      | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <code>snmp-server enable traps</code> | 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、簡易ネットワーク管理プロトコル (SNMP) の MAC アドレス変更通知トラップをイネーブルにするには、**snmp trap mac-notification change** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp trap mac-notification change {added | removed}
```

```
no snmp trap mac-notification change {added | removed}
```

## 構文の説明

|                |   |
|----------------|---|
| <b>added</b>   | MAC アドレスがこのインターフェイスに追加されると、MAC 通知トラップをイネーブルにします。  |
| <b>removed</b> | MAC アドレスがこのインターフェイスから削除されると、MAC 通知トラップをイネーブルにします。 |

## デフォルト

デフォルトでは、アドレス追加および削除に対するトラップは両方ともディセーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 change** コマンドを使用して、特定のインターフェイスの通知トラップをイネーブルにできますが、トラップが生成されるのは、**snmp-server enable traps mac-notification change** および **mac address-table notification change** グローバル コンフィギュレーション コマンドをイネーブルにした場合だけです。

## 例

次の例では、MAC アドレスがポートに追加されたときに MAC 通知トラップをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/2
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   |
|---|--|
| <b>clear mac address-table notification</b> | MAC アドレス通知グローバル カウンタをクリアします。   |
| <b>mac address-table notification</b>       | MAC アドレス通知機能をイネーブルにします。  |
| <b>show mac address-table notification</b>  | <b>interface</b> 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。 |
| <b>snmp-server enable traps</b>             | <b>mac-notification</b> キーワードが追加された場合に SNMP MAC 通知トラップを送信します。                      |

# spanning-tree backbonefast

BackboneFast 機能をイネーブルにします。デフォルト設定に戻すには、このコマンドの **no** 形式を使用し、**spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。

**spanning-tree backbonefast**

**no spanning-tree backbonefast**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

BackboneFast はディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

BackboneFast 機能は、Rapid PVST+ またはマルチ スパニングツリー (MST) モード用に設定できますが、スパニングツリー モードを PVST+ に変更するまでこの機能はディセーブル (非アクティブ) のままです。

スイッチのルート ポートまたはブロックされたポートが、指定スイッチから下位 BPDU を受信すると、BackboneFast が開始します。下位 BPDU は、ルートブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク (間接リンク) で障害が発生したことを意味します (つまり、指定スイッチとルートスイッチ間の接続が切断されています)。ルートスイッチへの代替パスがある場合に BackboneFast を使用すると、下位 BPDU を受信するインターフェイスの最大エージングタイムが期限切れになり、ブロックされたポートをただちにリスニングステートに移行できます。その後、BackboneFast はインターフェイスをフォワーディングステートに移行させます。詳細については、このリリースに対応するソフトウェア コンフィギュレーションガイドを参照してください。

間接リンク障害を検出し、スパニングツリーの再認識をより短時間で開始できるようにするには、サポートするすべてのスイッチで BackboneFast をイネーブルにします。

## 例

次の例では、スイッチ上で BackboneFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree backbonefast
```

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

## 関連コマンド

| コマンド                              | 説明                                 |
|-----------------------------------|------------------------------------|
| <b>show spanning-tree summary</b> | スパニングツリー インターフェイス ステートのサマリーを表示します。 |

# spanning-tree 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) を送受信しないようにするには、**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

|                |                                       |
|----------------|---------------------------------------|
| <b>disable</b> | 指定したインターフェイスで BPDU フィルタリングをディセーブルにします |
| <b>enable</b>  | 指定したインターフェイスで 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ モード、またはマルチ spanning ツリー (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す。



### 注意

BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上で spanning ツリーをディセーブルにすることと同じであり、spanning ツリー ループが発生することがあります。

すべての PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast 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 gigabitethernet1/1
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   |
|--|--|
| <code>show running-config</code>                               | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。                  |
| <code>spanning-tree portfast</code> (グローバル<br>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。 |
| <code>spanning-tree portfast</code> (インター<br>フェイス コンフィギュレーション) | 特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。  |

# spanning-tree bpduguard

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、**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                            | enable                            |
|-------|------------------------------------|-----------------------------------|
|       | 指定したインターフェイスで BPDU ガードをディセーブルにします。 | 指定したインターフェイスで 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            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが追加されました。 |

**使用上のガイドライン** インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービス プロバイダー ネットワーク内でインターフェイスがスパンニングツリー 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+ (RPVST+) モード、またはマルチ スパンニングツリー (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 対応インターフェイス上で BPDU ガードをグローバルにイネーブルにするには、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用します。

**spanning-tree bpduguard** インターフェイス コンフィギュレーション コマンドを使用すると、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドの設定を上書きできます。

**例** 次の例では、ポートで BPDU ガード機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/1
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   |
|--------|--|--|
|        | <code>show running-config</code>                           | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。                  |
|        | <code>spanning-tree portfast</code> (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。 |
|        | <code>spanning-tree portfast</code> (インターフェイス コンフィギュレーション) | 特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。  |

# spanning-tree cost

スパニングツリーの計算に使用するパス コストを設定します。ループが発生した場合、スパニングツリーがパス 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するように設定するには、**spanning-tree cost** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、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

|                            |  |
|----------------------------|--|
| <b>vlan <i>vlan-id</i></b> | (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。 |
| <b><i>cost</i></b>         | パス コストを指定します。指定できる範囲は 1 ~ 200000000 です。値が大きいほど、コストが高くなります。   |

## デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mb/s : 4
- 100 Mb/s : 19
- 10 Mb/s : 100

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

**spanning-tree vlan *vlan-id* cost *cost*** コマンドおよび **spanning-tree cost *cost*** コマンドの両方を使用してインターフェイスを設定する場合、**spanning-tree vlan *vlan-id* cost *cost*** コマンドが有効になります。

## 例

次の例では、ポートでパス コストを 250 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
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                                      |
|--|---|
| <code>show spanning-tree interface interface-id</code> | 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。          |
| <code>spanning-tree port-priority</code>               | インターフェイス 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 etherchannel guard misconfig

スイッチが EtherChannel の設定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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

スイッチが EtherChannel の設定に矛盾を検出すると、次のエラー メッセージが表示されます。

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in err-disable state.
```

設定に矛盾を持つ EtherChannel にあるスイッチ ポートを表示するには、**show interfaces status err-disabled** 特権 EXEC コマンドを使用します。リモート デバイスの EtherChannel 設定を確認するには、リモート デバイスで **show etherchannel summary** 特権 EXEC コマンドを使用します。

EtherChannel 設定矛盾によりポートが errdisable ステートの場合は、**errdisable recovery cause channel-misconfig** グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して、手動で再びイネーブルにすることができます。

## 例

次の例では、EtherChannel 設定矛盾のガード機能をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

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

## 関連コマンド

| コマンド   | 説明   |
|--|--|
| <b>errdisable recovery cause channel-misconfig</b> | EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。 |
| <b>show etherchannel summary</b>                   | チャネルの EtherChannel 情報を、チャネルグループ単位で 1 行のサマリーとして表示します。       |
| <b>show interfaces status err-disabled</b>         | 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

### 使用上のガイドライン

スイッチは、IEEE 802.1t スパニングツリー拡張をサポートします。以前スイッチ プライオリティに使用されたビットの一部を、現在は拡張システム ID (Per-VLAN Spanning-Tree Plus (PVST+) と Rapid PVST+ の VLAN 識別子、またはマルチ スパニングツリー (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 またはマルチ スパニングツリー 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  |
|---|---|
| <a href="#">show spanning-tree summary</a>  | 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。                |
| <a href="#">spanning-tree mst root</a>      | 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。 |
| <a href="#">spanning-tree vlan priority</a> | 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

選択したインターフェイスに関連付けられているすべての VLAN 上でルート ガードまたはループ ガードをイネーブルにするには、**spanning-tree guard** インターフェイス コンフィギュレーション コマンドを使用します。ルート ガードは、スパニングツリー ルート ポートまたはスイッチのルートへのパスになることが可能なインターフェイスを制限します。ループ ガードは、障害によって単一方向リンクが作成された場合に、代替ポートまたはルート ポートが指定ポートとして使用されないようにします。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**spanning-tree guard {loop | none | root}**

**no spanning-tree guard**

## 構文の説明

|             |                               |
|-------------|-------------------------------|
| <b>loop</b> | ループ ガードをイネーブルにします。            |
| <b>none</b> | 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。 |
| <b>root</b> | 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ (RPVST+) モード、またはマルチ スパニングツリー (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インターフェイスのすべての VLAN でディセーブルになります。このインターフェイスが **root-inconsistent** (ブロック) ステートの場合、インターフェイスはリスニング ステートに自動的に移行します。

UplinkFast 機能で使用するインターフェイスでは、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に (ブロック ステートの) バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能で使用するすべてのバックアップ インターフェイスが **root-inconsistent** (ブロック) ステートになり、フォワーディング ステートに移行できなくなります。スイッチが Rapid-PVST+ モードまたは MST モードで稼働している場合、UplinkFast 機能は使用できません。

ループ ガード機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid-PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートとして使用されることを防ぎます。スパニングツリーはルートポートまたは代替ポートでブリッジプロトコル データ ユニット (BPDU) を送信しません。スイッチが MST モードで動作している場合に、すべての MST インスタンスでインターフェイスがループガードによってブロックされているときは、BPDU は非境界インターフェイスからは送信されません。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ルート ガードまたはループ ガードをディセーブルにする場合は、**spanning-tree guard none** インターフェイス コンフィギュレーション コマンドを使用します。ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** インターフェイス コンフィギュレーション コマンドを使用します。

## 例

次の例では、指定のポートに関連付けられたすべての VLAN で、ループ ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/2
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 gigabitethernet1/2
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  |
|--|---|
| <b>show running-config</b>             | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>spanning-tree cost</b>              | 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。   |
| <b>spanning-tree loopguard default</b> | 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。                                       |
| <b>spanning-tree mst cost</b>          | MST の計算に使用するパス コストを設定します。   |
| <b>spanning-tree mst port-priority</b> | インターフェイス プライオリティを設定します。   |
| <b>spanning-tree mst root</b>          | 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。   |
| <b>spanning-tree port-priority</b>     | インターフェイス プライオリティを設定します。   |
| <b>spanning-tree vlan priority</b>     | 指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。   |

# spanning-tree link-type

インターフェイスのデュプレックス モードによって決定されるデフォルトのリンクタイプ設定を上書きし、フォワーディング ステートへの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、**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

|                       |   |
|-----------------------|---|
| <b>point-to-point</b> | インターフェイスのリンク タイプがポイントツーポイントであることを指定します。 |
| <b>shared</b>         | インターフェイスのリンク タイプが共有であることを指定します。         |

## デフォルト

スイッチは、デュプレックス モードからインターフェイスのリンク タイプを取得します。つまり、全二重インターフェイスはポイントツーポイント リンク、半二重インターフェイスは共有リンクであると見なされます。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

リンク タイプのデフォルト設定を上書きするには、**spanning-tree link-type** コマンドを使用します。たとえば半二重リンクは、マルチ スパニングツリー プロトコル (MSTP) または Rapid Per-VLAN Plus (Rapid-PVST+) スパニングツリー プロトコルが稼働中の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し、高速移行をイネーブルにできます。

## 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   |
|--|--|
| <code>clear spanning-tree detected-protocols</code>        | 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。 |
| <code>show spanning-tree interface interface-id</code>     | 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。  |
| <code>show spanning-tree mst interface interface-id</code> | 指定したインターフェイスの MST 情報を表示します。  |

# spanning-tree loopguard default

代替ポートまたはルートポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぐには、**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**spanning-tree loopguard default**

**no spanning-tree loopguard default**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

ループ ガードはディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ (RPVST+) モード、またはマルチ スパニングツリー (MST) モードで稼働している場合は、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 RPVST+ 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ブリッジプロトコルデータユニット (BPDU) を送信しません。スイッチが MST モードで動作している場合に、すべての MST インスタンスでインターフェイスがループ ガードによってブロックされているときは、BPDU は非境界インターフェイスからは送信されません。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ループ ガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でだけ動作します。

**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** インターフェイス コンフィギュレーション コマンドを使用します。

## 例

次の例では、ループ ガードをグローバルにイネーブルに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。

## ■ spanning-tree loopguard default

## 関連コマンド

| コマンド                                  | 説明  |
|---------------------------------------|---|
| <code>show running-config</code>      | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <code>spanning-tree guard loop</code> | 指定したインターフェイスに関連付けられたすべての VLAN で、ループ ガード機能をイネーブルにします。  |

# spanning-tree mode

スイッチで Per-VLAN Spanning-Tree Plus (PVST+)、Rapid PVST+ (RPVST+)、またはマルチ スパニング ツリー (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

|                   |  |
|-------------------|--|
| <b>mst</b>        | MST および高速スパニングツリー プロトコル (RSTP) をイネーブルにします (IEEE 802.1s および IEEE 802.1w に準拠)。 |
| <b>pvst</b>       | PVST+ をイネーブルにします (IEEE 802.1D に準拠)。  |
| <b>rapid-pvst</b> | Rapid PVST+ をイネーブルにします (IEEE 802.1w に準拠)。                                    |

## デフォルト

デフォルト モードは PVST+ です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 RPVST+、RPVST+、および MSTP に対応していますが、RPVST+、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 RPVST+ をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode rapid-pvst
```

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

## 関連コマンド

| コマンド                       | 説明   |
|----------------------------|--|
| <b>show running-config</b> | 現在の動作設定を表示します。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# spanning-tree mst configuration

MST リージョンを設定するマルチ スパニングツリー (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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**spanning-tree mst configuration** コマンドを入力すると、MST コンフィギュレーション モードが開始します。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **abort** : 設定変更を適用しないで、MST リージョン コンフィギュレーション モードを終了します。
- **exit** : MST リージョン コンフィギュレーション モードを終了し、すべての設定変更を適用します。
- **instance instance-id vlan vlan-range** : VLAN を MST インスタンスにマッピングします。  
*instance-id* に指定できる範囲は 1 ~ 4094 です。*vlan-range* に指定できる範囲は 1 ~ 4094 です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。
- **name name** : 設定名を設定します。*name* ストリングには最大 32 文字使用でき、大文字と小文字が区別されます。
- **no** : **instance**、**name**、および **revision** コマンドを無視するか、またはデフォルト設定に戻します。
- **private-vlan** : 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、このコマンドはサポートされません。
- **revision version** : コンフィギュレーション リビジョン番号を設定します。指定できる範囲は 0 ~ 65535 です。
- **show [current | pending]** : 現在のまたは保留中の MST リージョンの設定を表示します。

MST モードでは、スイッチは最大 65 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 リージョン内に存在する場合、同じ VLAN マッピング、同じコンフィギュレーション リビジョン番号、および同じ名前が設定されている必要があります。

## 例

次の例は、MST コンフィギュレーション モードを開始し、VLAN 10 ~ 20 を MSTI 1 にマッピングし、領域に **region1** という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0          1-9,21-4094
1          10-20
-----

Switch(config-mst)# exit
Switch(config)#
```

次の例では、VLAN 1 ~ 100 を、すでに同じ VLAN がマッピングされている場合でも、インスタンス 2 に追加し、ここでインスタンス 2 にマッピングした VLAN 40 ~ 60 を CIST インスタンスに移動します。その後、インスタンス 10 に VLAN 10 を追加し、インスタンス 2 にマッピングされているすべての VLAN を削除して、それらを CIST インスタンスにマッピングする方法を示します。

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

設定を確認するには、**show pending MST** コンフィギュレーション コマンドを入力します。

## 関連コマンド

| コマンド  | 説明                  |
|---|---------------------|
| <b>show spanning-tree mst configuration</b> | MST リージョンの設定を表示します。 |

# spanning-tree mst cost

マルチ スパニングツリー (MST) の計算に使用するパス コストを設定するには、**spanning-tree mst cost** インターフェイス コンフィギュレーション コマンドを使用します。ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**spanning-tree mst instance-id cost cost**

**no spanning-tree mst instance-id cost**

## 構文の説明

|                    |   |
|--------------------|---|
| <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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

## 例

次の例では、インスタンス 2 および 4 に関連付けられたポートにパス コストとして 250 を設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

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

## 関連コマンド

| コマンド  | 説明                                       |
|---|--|
| <code>show spanning-tree mst interface <i>interface-id</i></code> | 指定したインターフェイスの MST 情報を表示します。              |
| <code>spanning-tree mst port-priority</code>                      | インターフェイス プライオリティを設定します。                  |
| <code>spanning-tree mst priority</code>                           | 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 forward-time

すべてのマルチ スパニングツリー (MST) インスタンスの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            |
|        | 15.0(1)EY | このコマンドが追加されました。 |

使用上のガイドライン **spanning-tree mst forward-time** コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例 次の例では、すべての MST インスタンスについて、スパニングツリーの転送遅延時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst forward-time 18
```

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

|        |                                     |  |
|--------|-------------------------------------|--|
| 関連コマンド | コマンド                                | 説明   |
|        | <b>show spanning-tree mst</b>       | MST 情報を表示します。  |
|        | <b>spanning-tree mst hello-time</b> | 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 ブリッジ プロトコル データ ユニット (BPDU) の間隔を設定します。 |
|        | <b>spanning-tree mst max-age</b>    | 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。                                       |
|        | <b>spanning-tree mst max-hops</b>   | 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 メッセージで送信される hello ブリッジ プロトコル データ ユニット (BPDU) の間隔を設定するには、**spanning-tree mst hello-time** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**spanning-tree mst hello-time** *seconds*

**no spanning-tree mst hello-time**

## 構文の説明

*seconds* ルートスイッチ コンフィギュレーション メッセージから送信される hello BPDU の間隔です。指定できる範囲は 1 ~ 10 秒です。

## デフォルト

デフォルト値は 2 秒です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**spanning-tree mst max-age** *seconds* グローバル コンフィギュレーション コマンドを設定した後に、スイッチが指定された間隔の間にルートスイッチから BPDU を受信しなかった場合は、スパニングツリー トポロジが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

**spanning-tree mst hello-time** コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

## 例

次の例では、すべてのマルチ スパニングツリー (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                                    |
|---------------------------------------|---------------------------------------|
| <b>show spanning-tree mst</b>         | MST 情報を表示します。                         |
| <b>spanning-tree mst forward-time</b> | 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。      |
| <b>spanning-tree mst max-age</b>      | 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。 |
| <b>spanning-tree mst max-hops</b>     | 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 スイッチからメッセージを受信する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 スイッチからブリッジプロトコル データ ユニット (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。デフォルト設定に戻すには、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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**spanning-tree mst max-age seconds** グローバル コンフィギュレーション コマンドを設定した後に、スイッチが指定された間隔の間にルート スイッチから BPDU を受信しなかった場合は、スパニングツリー トポロジが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

**spanning-tree mst max-age** コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

## 例

次の例では、すべてのマルチ スパニングツリー (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   |
|---------------------------------------|--|
| <b>show spanning-tree mst</b>         | MST 情報を表示します。                                      |
| <b>spanning-tree mst forward-time</b> | 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。                   |
| <b>spanning-tree mst hello-time</b>   | 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。 |
| <b>spanning-tree mst max-hops</b>     | 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

ブリッジプロトコルデータユニット (BPDU) が廃棄されて、インターフェイス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 カウントを設定します。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、**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。

**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            |
|-----------|-----------------|
| 15.0(1)EY | 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、すべてのマルチ スパニングツリー (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   |
|---------------------------------------|--|
| <b>show spanning-tree mst</b>         | MST 情報を表示します。                                      |
| <b>spanning-tree mst forward-time</b> | 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。                   |
| <b>spanning-tree mst hello-time</b>   | 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。 |
| <b>spanning-tree mst max-age</b>      | スパニングツリーがルート スイッチからメッセージを受信する間隔を設定します。             |

# spanning-tree mst port-priority

インターフェイス プライオリティを設定するには、**spanning-tree mst port-priority** インターフェイス コンフィギュレーション コマンドを使用します。ループが発生した場合、マルチ スパニングツリー プロトコル (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            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが追加されました。 |

**使用上のガイドライン** 最初に選択されるインターフェイスには高いプライオリティ値 (小さい数値) を割り当て、最後に選択されるインターフェイスには低いプライオリティ値 (高い数値) を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が付けられている場合、マルチ スパニングツリー (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 gigabitethernet1/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

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

## 関連コマンド

| コマンド   | 説明                                       |
|--|--|
| <code>show spanning-tree mst interface interface-id</code> | 指定したインターフェイスの MST 情報を表示します。              |
| <code>spanning-tree mst cost</code>                        | MST の計算に使用するパス コストを設定します。                |
| <code>spanning-tree mst priority</code>                    | 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

先行標準のブリッジプロトコルデータユニット (BPDU) だけを送信するようにポートを設定するには、**spanning-tree mst pre-standard** インターフェイス 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。

## デフォルト

デフォルトのステートは、先行標準ネイバーの自動検出です。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

ポートでは、先行標準と標準の両方の BPDU を受け入れることができます。ネイバータイプが不一致の場合、Common and Internal Spanning Tree (CIST) だけがこのインターフェイスで実行されます。



(注)

スイッチのポートが、先行標準の Cisco IOS ソフトウェアを実行しているスイッチに接続されている場合には、ポートに対して **spanning-tree mst pre-standard** インターフェイス コンフィギュレーション コマンドを使用する必要があります。先行標準 BPDU だけを送信するようにポートを設定していない場合、マルチ STP (MSTP) のパフォーマンスが低下することがあります。

自動的に先行標準ネイバーを検出するようにポートが設定されている場合、**show spanning-tree mst** コマンドに **prestandard** フラグが常に表示されます。

## 例

次の例では、先行標準 BPDU だけを送信するようにポートを設定する方法を示します。

```
Switch(config-if)# spanning-tree mst pre-standard
```

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

## 関連コマンド

| コマンド                                      | 説明  |
|---|---|
| <b>show spanning-tree mst instance-id</b> | prestandard フラグなど、指定されたインターフェイスの Multiple Spanning-Tree (MST) 情報を表示します。 |

# spanning-tree mst priority

指定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

|                    |   |
|--------------------|---|
| <b>instance-id</b> | 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。   |
| <b>priority</b>    | 指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。この設定は、スイッチがルート スイッチとして選択される可能性を左右します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。<br><br>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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 例

次の例では、マルチ スパニングツリー (MST) インスタンス 20 ~ 21 のスパニングツリー プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

設定を確認するには、**show spanning-tree mst instance-id** 特権 EXEC コマンドを入力します。

## 関連コマンド

| コマンド                                      | 説明                          |
|---|-----------------------------|
| <b>show spanning-tree mst instance-id</b> | 指定したインターフェイスの MST 情報を表示します。 |
| <b>spanning-tree mst cost</b>             | MST の計算に使用するパス コストを設定します。   |
| <b>spanning-tree mst port-priority</b>    | 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マルチ スパニングツリー (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。                                 |
| <b>primary</b>               | このスイッチを強制的にルート スイッチに設定します。  |
| <b>secondary</b>             | 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。  |
| <i>diameter 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。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。  |
| <i>hello-time 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 ブリッジプロトコル データ ユニット (BPDU) 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**spanning-tree mst instance-id root** コマンドは、バックボーン スイッチだけで使用してください。

**spanning-tree mst instance-id root** コマンドを入力すると、ソフトウェアはこのスイッチをスパニングツリー インスタンスのルートに設定するのに十分なプライオリティを設定しようとします。拡張システム ID がサポートされているため、スイッチはインスタンスのスイッチ プライオリティを 24576 に設定します (この値によってこのスイッチが指定されたインスタンスのルートになる場合)。指定されたインスタンスのルート スイッチに、24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します (4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です)。

**spanning-tree mst instance-id root secondary** コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアはスイッチ プライオリティをデフォルト値 (32768) から 28672 に変更します。ルート スイッチに障害が発生した場合は、このスイッチが次のルート スイッチになります (ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティである 32768 を使用しているため、ルート スイッチになる可能性が低い場合)。

**例**

次の例では、スイッチをインスタンス 10 のルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

次の例では、スイッチをインスタンス 10 のセカンダリ ルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree mst instance-id** 特権 EXEC コマンドを入力します。

**関連コマンド**

| コマンド                                      | 説明  |
|---|---|
| <b>show spanning-tree mst instance-id</b> | 指定したインスタンスの MST 情報を表示します。                             |
| <b>spanning-tree mst forward-time</b>     | 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。                      |
| <b>spanning-tree mst hello-time</b>       | 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。 |
| <b>spanning-tree mst max-age</b>          | 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。                |
| <b>spanning-tree mst max-hops</b>         | 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、**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

|                            |  |
|----------------------------|--|
| <b>vlan <i>vlan-id</i></b> | (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。 |
| <b><i>priority</i></b>     | 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

変数 *vlan-id* を省略した場合、このコマンドは VLAN 1 に関連付けられたスパンニングツリー 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。このインターフェイスを VLAN に割り当てると、設定が有効になります。

**spanning-tree vlan *vlan-id* port-priority *priority*** コマンドおよび **spanning-tree port-priority *priority*** コマンドの両方を使用してインターフェイスを設定する場合、**spanning-tree vlan *vlan-id* port-priority *priority*** コマンドが有効になります。

## 例

次の例では、ループが発生した場合にポートがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet1/2
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                                      |
|--|---|
| <code>show spanning-tree interface interface-id</code> | 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。          |
| <code>spanning-tree cost</code>                        | 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。           |
| <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 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、PortFast 対応インターフェイス上で BPDU ガード機能フィルタを、またはすべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにするには、**spanning-tree portfast** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree portfast {bpdudfilter default | bpduguard default | default}
```

```
no spanning-tree portfast {bpdudfilter default | bpduguard default | default}
```

## 構文の説明

|                            |   |
|----------------------------|---|
| <b>bpdudfilter default</b> | PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにし、エンドステーションに接続されたスイッチ インターフェイスでの BPDU の送受信を防ぎます。   |
| <b>bpduguard default</b>   | PortFast 対応インターフェイス上で BPDU ガード機能をグローバルにイネーブルにし、BPDU を受信するインターフェイスを <b>errdisable</b> ステートにします。  |
| <b>default</b>             | すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにします。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。 |

## デフォルト

BPDU フィルタリング、BPDU ガード、および PortFast 機能は、個別に設定しない限り、すべてのインターフェイスでディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

BPDU フィルタリング機能を使用すると、スイッチ インターフェイスでの BPDU の送受信を禁止できます。BPDU ガード機能は、BPDU を受信する PortFast 対応インターフェイスを **errdisable** ステートにします。

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ (RPVST+) モード、またはマルチ スパニングツリー (MST) モードで稼働している場合は、これらの機能をイネーブルにできます。

PortFast 対応インターフェイス (PortFast 動作ステートのインターフェイス) 上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast 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。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。スイッチ インターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で

BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは、PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bdpufilter** インターフェイス コンフィギュレーション コマンドを使用します。

**注意**

BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

PortFast 動作ステートのインターフェイス上で BPDU ガードをグローバルにイネーブルにするには、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用します。有効な設定では、PortFast 対応インターフェイスは BPDU を受信しません。PortFast 対応インターフェイスが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってインターフェイスは **errdisable** ステートになります。インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービス プロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bdpuguard** インターフェイス コンフィギュレーション コマンドを使用します。

すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにするには、**spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用します。PortFast は、エンドステーションに接続するインターフェイスに限って設定します。そうしないと、予期しないトポロジープが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。リンクが確立すると、PortFast 対応インターフェイスは標準の転送遅延時間の経過を待たずに、ただちにスパニングツリー フォワーディング ステートに移行します。

**spanning-tree portfast default** グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用します。**no spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用すると、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して個別に設定した場合を除き、すべてのインターフェイス上で PortFast をディセーブルにできます。

**例** 次の例では、BPDU フィルタリング機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast bpduguard 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。

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

## 関連コマンド

| コマンド   | 説明  |
|--|---|
| <code>show running-config</code>                           | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <code>spanning-tree bpdufilter</code>                      | インターフェイスが BPDU を送受信しないようにします。   |
| <code>spanning-tree bpduguard</code>                       | BPDU を受信したインターフェイスを、errdisable ステートにします。  |
| <code>spanning-tree portfast (インターフェイス コンフィギュレーション)</code> | 対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。   |

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

関連するすべての VLAN 内のインターフェイス上で 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 コマンドを使用します。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**spanning-tree portfast [disable | trunk]**

**no spanning-tree portfast**

## 構文の説明

|                |  |
|----------------|--|
| <b>disable</b> | (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。  |
| <b>trunk</b>   | (任意) トランキング インターフェイスの PortFast 機能をイネーブルにします。 |

## デフォルト

すべてのインターフェイスで PortFast 機能はディセーブルですが、ダイナミック アクセス ポートでは自動的にイネーブルになります。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

この機能は、エンドステーションに接続するインターフェイスに限って使用します。そうしないと、予期しないトポロジ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+ (RPVST+) モード、またはマルチ スパニングツリー (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せん。

この機能はインターフェイス上のすべての VLAN に影響します。

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、ただちにスパニングツリー フォワーディング ステートに移行します。

**spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにできます。ただし、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して、グローバル設定を上書きできます。

**spanning-tree portfast default** グローバル コンフィギュレーション コマンドを設定する場合は、**spanning-tree portfast disable** インターフェイス コンフィギュレーション コマンドを使用して、トランク インターフェイス以外のインターフェイス上で PortFast 機能をディセーブルにできます。

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

## 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 gigabitethernet1/2
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   |
|---|--|
| <b>show running-config</b>                        | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。                  |
| <b>spanning-tree bpdupfilter</b>                  | インターフェイスでのブリッジプロトコルデータユニット (BPDU) の送受信を禁止します。  |
| <b>spanning-tree bpduguard</b>                    | BPDU を受信したインターフェイスを、errdisable ステートにします。   |
| <b>spanning-tree portfast (グローバル コンフィギュレーション)</b> | PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。 |

# spanning-tree transmit hold-count

毎秒送信されるブリッジプロトコル データ ユニット (BPDU) の数を設定するには、**spanning-tree transmit hold-count** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**spanning-tree transmit hold-count** [*value*]

**no spanning-tree transmit hold-count** [*value*]

## 構文の説明

*value* (任意) 秒送信される BPDU 数。指定できる範囲は 1 ~ 20 です。

## デフォルト

デフォルト値は 6 です。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

RPVST+ モードの場合、送信保留カウンターの値を増やすと、CPU 利用率に重大な影響を及ぼす可能性があります。この値を減らすと、コンバージェンスの速度が低下します。デフォルト設定を使用することを推奨します。

## 例

次の例では、伝送ホールド カウントを 8 に設定する方法を示します。

```
Switch(config)# spanning-tree transmit hold-count 8
```

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

## 関連コマンド

| コマンド                                   | 説明  |
|--|---|
| <a href="#">show spanning-tree mst</a> | 伝送ホールド カウントを含む、マルチ スパニングツリー (MST) のリージョン設定およびステータスを表示します。 |

# spanning-tree uplinkfast

リンクやスイッチに障害が発生した場合、またはスパニングツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択するには、**spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*]

**no spanning-tree uplinkfast** [**max-update-rate**]

## 構文の説明

**max-update-rate** *pkts-per-second* (任意) 更新パケット送信時の 1 秒あたりのパケット数です。指定できる範囲は 0 ~ 32000 です。

## デフォルト

UplinkFast はディセーブルです。  
更新速度は 150 パケット/秒です。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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、アクセス スイッチ上で使用します。

UplinkFast 機能は、Rapid PVST+ (RPVST+) モードまたはマルチ スパニングツリー (MST) モードで設定できますが、スパニングツリー モードを PVST+ に変更するまでこの機能はディセーブル (非アクティブ) のままです。

UplinkFast をイネーブルにすると、スイッチ全体に対してイネーブルになります。VLAN 単位でイネーブルにすることはできません。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されません。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します (パス コストを 3000 以上の値に変更した場合、パス コストは変更されません)。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

ルート ポートに障害が発生していることがスパニングツリーで検出されると、UplinkFast はスイッチをただちに代替ルート ポートに変更して、新しいルート ポートを直接フォワーディング ステートに移行させます。この間、トポロジ変更通知が送信されます。

UplinkFast 機能で使用するインターフェイスでは、ルートガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルートポートになります。しかし、同時にルートガードもイネーブルになっていた場合は、UplinkFast 機能で使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

max-update-rate を 0 に設定すると、ステーションを学習するフレームが生成されず、接続の切断後、スパニングツリー トポロジのコンバージェンスに要する時間が長くなります。

#### 例

次の例では、UplinkFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree uplinkfast
```

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

#### 関連コマンド

| コマンド  | 説明                                 |
|---|------------------------------------|
| <a href="#">show spanning-tree summary</a>      | 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。 |
| <a href="#">spanning-tree vlan root primary</a> | このスイッチを強制的にルート スイッチに設定します。         |

# spanning-tree vlan

毎 VLAN 単位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

|                                     |  |
|-------------------------------------|--|
| <i>vlan-id</i>                      | 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。  |
| <b>forward-time</b> <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。   |
| <b>hello-time</b> <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 ブリッジ プロトコル データ ユニット (BPDU) の間隔を設定します。指定できる範囲は 1 ~ 10 秒です。   |
| <b>max-age</b> <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。   |
| <b>priority</b> <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。<br><br>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。 |
| <b>root primary</b>                 | (任意) このスイッチを強制的にルート スイッチにします。  |
| <b>root secondary</b>               | (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。  |
| <b>diameter</b> <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            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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 をディセーブルにすると、VLAN はスパニングツリー トポロジへの参加を停止します。管理上のダウン状態のインターフェイスは、ダウン状態のままです。受信した BPDU は、他のマルチキャストフレームと同様に転送されます。STP がディセーブルの場合、VLAN はループの検出や禁止を行いません。

現在アクティブではない VLAN 上で STP をディセーブルにし、この変更を確認するには、**show running-config** または **show spanning-tree vlan vlan-id** 特権 EXEC コマンドを使用します。設定は、VLAN がアクティブである場合に有効となります。

STP をディセーブルにするか、再びイネーブルにすると、ディセーブルまたはイネーブルにする VLAN 範囲を指定できます。

VLAN をディセーブルにしてからイネーブルにした場合、その VLAN に割り当てられていたすべての VLAN は引き続きメンバとなります。ただし、すべてのスパニングツリーブリッジパラメータは元の設定（VLAN がディセーブルになる直前の設定）に戻ります。

インターフェイスが割り当てられていない VLAN 上で、スパニングツリー オプションをイネーブルにできます。インターフェイスを VLAN に割り当てると、設定が有効になります。

**max-age seconds** を設定すると、スイッチが指定された間隔の間にルートスイッチから BPDU を受信しなかった場合は、スパニングツリー トポロジが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

**spanning-tree vlan vlan-id root** コマンドは、バックボーンスイッチだけで使用してください。

**spanning-tree vlan vlan-id root** コマンドを入力すると、ソフトウェアは各 VLAN の現在のルートスイッチのスイッチプライオリティを確認します。拡張システム ID がサポートされているため、スイッチは指定された VLAN のスイッチプライオリティを 24576 に設定します（この値によってこのスイッチが指定された VLAN のルートになる場合）。指定された VLAN のルートスイッチに 24576 に満たないスイッチプライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチプライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビットスイッチプライオリティの最下位ビットの値です）。

**spanning-tree vlan vlan-id root secondary** コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアはスイッチプライオリティをデフォルト値（32768）から 28672 に変更します。ルートスイッチに障害が発生した場合は、このスイッチが次のルートスイッチになります（ネットワーク内の他のスイッチがデフォルトのスイッチプライオリティである 32768 を使用しているため、ルートスイッチになる可能性が低い場合）。

### 例

次の例では、VLAN 5 上で STP をディセーブルにする方法を示します。

```
Switch(config)# no spanning-tree vlan 5
```

設定を確認するには、**show spanning-tree** 特権 EXEC コマンドを入力します。このインスタンスのリストに、VLAN 5 は表示されません。

次の例では、VLAN 20 と VLAN 25 のスパニングツリーについて、転送遅延時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

## spanning-tree vlan

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 **max-age** パラメータを 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   |
|--|--|
| <b>show spanning-tree vlan</b>                       | スパニングツリー情報を表示します。  |
| <b>spanning-tree cost</b>                            | 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。  |
| <b>spanning-tree guard</b>                           | 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。  |
| <b>spanning-tree port-priority</b>                   | インターフェイス プライオリティを設定します。  |
| <b>spanning-tree portfast (グローバル コンフィギュレーション)</b>    | 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。 |
| <b>spanning-tree portfast (インターフェイス コンフィギュレーション)</b> | 対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。  |
| <b>spanning-tree uplinkfast</b>                      | UplinkFast 機能をイネーブルにし、新しいルート ポートを短時間で選択できるようにします。  |

# speed

10/100 Mb/s または 10/100/1000 Mb/s ポートの速度を指定するには、**speed** インターフェイス コンフィギュレーション コマンドを使用します。ポートをデフォルト値に戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

```
speed {10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate}
no speed
```

## 構文の説明

|                    |   |
|--------------------|---|
| <b>10</b>          | 10 Mb/s を指定します。   |
| <b>100</b>         | 100 Mb/s を指定します。  |
| <b>1000</b>        | 1000 Mb/s を指定します。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。  |
| <b>auto</b>        | リンクのもう一方の終焉のポートを基準にして自動的に速度を検出します。 <b>10</b> 、 <b>100</b> 、または <b>1000</b> キーワードと <b>auto</b> 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。 |
| <b>nonegotiate</b> | 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 <b>nonegotiate</b> 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

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**) 速度を設定できません。

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およびデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

**例**

次の例では、ポートの速度を 100 Mb/s に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# speed 100
```

次の例では、10 Mb/s だけで自動ネゴシエートするようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# speed auto 10
```

次の例では、10 Mb/s または 100 Mb/s だけで自動ネゴシエートするようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
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  |
|------------------------|---|
| <b>duplex</b>          | デュプレックス モードの動作を指定します。                     |
| <b>show interfaces</b> | すべてのインターフェイスまたは特定のインターフェイスに対する統計情報を表示します。 |

# srr-queue bandwidth limit

ポートの最大出力を制限します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。  
**srr-queue bandwidth limit** インターフェイス コンフィギュレーション コマンドを使用します。

**srr-queue bandwidth limit** *weight1*

**no srr-queue bandwidth limit**

## 構文の説明

*weight1* 制限されるポート速度のパーセンテージ。指定できる範囲は 10 ~ 90 です。

## デフォルト

ポートはレート制限されておらず、100% に設定されます。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドを 80% に設定した場合、ポートは 20% の時間はアイドル状態になります。ライン レートは接続速度の 80% に下がります。ただし、ハードウェアはライン レートを 6% 単位で調整しているため、この値は厳密ではありません。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの Quality of Service (QoS) ソリューションを満たさないと判断した場合に限り、設定を変更することができます。

## 例

次の例では、ポートを 80 Mb/s に制限する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth limit 80
```

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

## 関連コマンド

| コマンド                                      | 説明   |
|---|--|
| <b>mls qos queue-set output buffers</b>   | バッファをキューセットに割り当てます。  |
| <b>mls qos srr-queue output cos-map</b>   | サービス クラス (CoS) 値を出力キュー、またはキューとしきい値 ID にマッピングします。                     |
| <b>mls qos srr-queue output dscp-map</b>  | DiffServ コード ポイント (DSCP) 値を出力キュー、またはキューとしきい値 ID にマッピングします。           |
| <b>mls qos queue-set output threshold</b> | 重み付けテール ドロップ (WTD) しきい値を設定し、バッファの可用性を保証して、キューセットに対する最大メモリ割り当てを設定します。 |
| <b>queue-set</b>                          | ポートをキューセットにマッピングします。   |
| <b>show mls qos interface queueing</b>    | QoS 情報を表示します。  |
| <b>srr-queue bandwidth shape</b>          | シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。        |
| <b>srr-queue bandwidth share</b>          | 共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。                |

# srr-queue bandwidth shape

シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キューの帯域幅のシェーピングをイネーブルにするには、**srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**srr-queue bandwidth shape weight1 weight2 weight3 weight4**

**no srr-queue bandwidth shape**

## 構文の説明

*weight1 weight2 weight3 weight4* シェーピングされるポートのパーセンテージを指定する重みを割り当てます。インパース比 ( $1/\text{weight}$ ) は、このキューのシェーピング帯域幅を指定します。各値はスペースで区切ります。指定できる範囲は 0 ~ 65535 です。

## デフォルト

weight1 は 25 に設定されています。weight2、weight3、および weight4 は 0 に設定されています。また、このキューは共有モードです。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

シェーピング モードでは、キューには帯域幅が割合で保証され、この総量までにレート制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を超えて使用できません。パースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。

シェーピング モードは、共有モードを無効にします。

**srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用してシェーピングされたキューの重みを 0 に設定すると、このキューは共有モードで参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。

同じポートのキューをシェーピングと共有の両方に設定する場合、最小のキューをシェーピングに設定します。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

## 例

次の例では、同じポートのキューをシェーピングと共有の両方に設定する方法を示します。キュー 2、3、4 の重み比が 0 に設定されているので、これらのキューは共有モードで動作します。キュー 1 の帯域幅の重みは 1/8 で、これは 12.5% です。キュー 1 はこの帯域幅が保証され、またこの帯域幅までに

## ■ srr-queue bandwidth shape

制限されています。他のキューにトラフィックがなくアイドル状態であっても、他のキューにスロットを拡張しません。キュー 2、3、4 は共有モードで、キュー 1 の設定は無視されます。共有モードのキューに割り当てられた帯域幅比は、4/(4+4+4) で、これは 33% です。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <a href="#">mls qos queue-set output buffers</a>                          | バッファをキューセットに割り当てます。   |
| <a href="#">mls qos srr-queue output cos-map</a>                          | Class of Service (CoS) 値を出力キュー、またはキューとしきい値 ID にマッピングします。                                    |
| <a href="#">mls qos srr-queue output dscp-map</a>                         | DiffServ コードポイント (DSCP) 値を出力キュー、またはキューとしきい値 ID にマッピングします。                                   |
| <a href="#">mls qos queue-set output threshold</a>                        | 重み付けテールドロップ (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当てを設定します。                          |
| <a href="#">priority-queue queue-set</a>                                  | ポート上で出力緊急キューをイネーブルにします。<br>ポートをキューセットにマッピングします。   |
| <a href="#">show mls qos interface queueing srr-queue bandwidth share</a> | Quality of Service (QoS) 情報を表示します。<br>共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。 |

# srr-queue bandwidth share

共有する重みを割り当て、ポートにマッピングされた4つの出力キューの帯域幅の共有をイネーブルにするには、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドを使用します。重み比は、シェイプド ラウンド ロビン (SRR) スケジューラが各キューからパケットを取り出す頻度の比率です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
srr-queue bandwidth share weight1 weight2 weight3 weight4
```

```
no srr-queue bandwidth share
```

## 構文の説明

|  |  |
|--|--|
| <i>weight1 weight2 weight3 weight4</i> | SRR スケジューラがパケットを取り出す頻度の比率。各値はスペースで区切ります。指定できる範囲は1～255です。 |
|--|--|

## デフォルト

weight1、weight2、weight3 および weight4 は 25 に設定されています (各キューに帯域幅の 1/4 を割り当て)。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

各重みの絶対値は意味がないので、パラメータ比だけを使用します。

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、キューが空でリンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。

**srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用してシェーピングされたキューの重みを 0 に設定すると、このキューは SRR 共有モードで参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで指定されたキューの重みが有効になります。

同じポートのキューをシェーピングと共有の両方に設定する場合、最小のキューをシェーピングに設定します。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

## 例

次の例では、出力ポートで稼働する SRR スケジューラの重み比を設定する方法を示します。キュー 4 つを使用します。共有モードの各キューに割り当てられた帯域幅の比率は、1/ (1+2+3+4)、2/ (1+2+3+4)、3/ (1+2+3+4)、4/ (1+2+3+4) で、これは、キュー 1、2、3、4 それぞれに対して 10%、20%、30%、40% です。キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet1/1
```

## ■ srr-queue bandwidth share

```
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

## 関連コマンド

| コマンド                                      | 説明  |
|---|---|
| <b>mls qos queue-set output buffers</b>   | バッファをキューセットに割り当てます。   |
| <b>mls qos srr-queue output cos-map</b>   | Class of Service (CoS) 値を出力キュー、またはキューとしきい値 ID にマッピングします。            |
| <b>mls qos srr-queue output dscp-map</b>  | DiffServ コード ポイント (DSCP) 値を出力キュー、またはキューとしきい値 ID にマッピングします。          |
| <b>mls qos queue-set output threshold</b> | 重み付けテール ドロップ (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当てを設定します。 |
| <b>priority-queue</b>                     | ポート上で出力緊急キューをイネーブルにします。   |
| <b>queue-set</b>                          | ポートをキューセットにマッピングします。  |
| <b>show mls qos interface queueing</b>    | Quality of Service (QoS) 情報を表示します。                                  |
| <b>srr-queue bandwidth shape</b>          | シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。       |

# storm-control

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、インターフェイスのしきい値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

|                                |  |
|--------------------------------|--|
| <b>broadcast</b>               | インターフェイスのブロードキャスト ストーム制御をイネーブルにします。  |
| <b>multicast</b>               | 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。  |
| <b>unicast</b>                 | 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。   |
| <b>level level level-low</b>   | <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"> <li><b>level</b> : 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 <b>level</b> 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。</li> <li><b>level-low</b> : (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。</li> </ul>                                       |
| <b>level bps bps [bps-low]</b> | <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"> <li><b>bps</b> : 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 <b>bps</b> 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。</li> <li><b>bps-low</b> : (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。</li> </ul> <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す。</p>  |
| <b>level pps pps [pps-low]</b> | <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"> <li><b>pps</b> : 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 <b>pps</b> 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。</li> <li><b>pps-low</b> : (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。</li> </ul> <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す。</p> |

|                        |   |
|------------------------|---|
| <b>action</b>          | 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、簡易ネットワーク管理プロトコル (SNMP) トラップを送信しません。  |
| <b>shutdown   trap</b> | キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>shutdown</b> : ストームの間、ポートをディセーブルにします。</li> <li>• <b>trap</b> : ストーム発生時に、SNMP トラップを送信します。</li> </ul> |

**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            |
|-----------|-----------------|
| 15.0(1)EY | 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、ブリッジプロトコルデータユニット (BPDU)、Cisco Discovery Protocol (CDP) フレームのような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、スイッチでは **Open Shortest Path First (OSPF)** のようなルーティングアップデートと、正規のマルチキャストデータトラフィックは区別されないため、両方のトラフィックタイプがブロックされます。

**trap** および **shutdown** オプションは、互いに独立しています。

パケットストームが検出されたときにシャットダウンを行う（ストームの間、ポートが **errdisable** になる）ようにアクションを設定する場合、インターフェイスをこのステートから解除するには **no shutdown** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**shutdown** アクションを指定しない場合、アクションを **trap**（ストーム検出時にスイッチがトラップを生成する）に指定してください。

ストームが発生し、実行されるアクションがトラフィックのフィルタリングである場合、下限抑制レベルが指定されていないと、トラフィックレートが上限抑制レベルより低くなるまでスイッチはすべてのトラフィックをブロックします。下限抑制レベルが指定されている場合、トラフィックレートがこのレベルより低くなるまでスイッチはトラフィックをブロックします。



(注)

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ブロードキャスト ストームが発生し、実行されるアクションがトラフィックのフィルタである場合、スイッチはブロードキャスト トラフィックだけをブロックします。

詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、75.5% の上限抑制レベルでブロードキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control broadcast level 75.5
```

次の例では、87% の上限抑制レベルと 65% の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control unicast level 87 65
```

次の例では、2000 パケット/秒の上限抑制レベルと 1000 パケット/秒の下限抑制レベルのポートでマルチキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

次の例では、ポートで shutdown アクションをイネーブルにする方法を示します。

```
Switch(config-if)# storm-control action shutdown
```

関連コマンド

| コマンド                               | 説明  |
|------------------------------------|---|
| <a href="#">show storm-control</a> | 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 access

スタティック アクセスまたはダイナミック アクセス ポートとしてポートを設定するには、**switchport access** インターフェイス コンフィギュレーション コマンドを使用します。アクセス モードをスイッチのデフォルト VLAN にリセットするには、このコマンドの **no** 形式を使用します。

```
switchport access vlan {vlan-id | dynamic}
```

```
no switchport access vlan
```

## 構文の説明

|                            |  |
|----------------------------|--|
| <b>vlan</b> <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。   |
| <b>vlan</b> <b>dynamic</b> | VLAN メンバーシップ ポリシー サーバ (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、新しい MAC アドレスを受信するたびに VMPS サーバに送信して、ダイナミック アクセス ポートに割り当てられる VLAN の名前を取得します。すでに、ポートには VLAN が割り当てられていて、送信元が VMPS によって承認されている場合、スイッチはパケットを該当する VLAN に転送します。 |

## デフォルト

デフォルトのアクセス VLAN およびトランク インターフェイス ネイティブ VLAN は、プラットフォームまたはインターフェイス ハードウェアに対応したデフォルト VLAN です。

ダイナミック アクセス ポートは、最初は何の 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

スイッチポートのモードが、**access** に設定されている場合、ポートは指定の VLAN のメンバとして動作します。**dynamic** として設定されている場合、ポートは受信した着信パケットに基づいて、VLAN 割り当ての検出を開始します。

**no switchport access** コマンドは、アクセス モード VLAN をデバイスの適切なデフォルト VLAN にリセットします。

**switchport access vlan** コマンドを有効にするには、事前にポートをアクセス モードにする必要があります。

アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。

ポートをダイナミックとして設定するには、事前に VMPS サーバ (Catalyst 6500 シリーズ スイッチなど) を設定する必要があります。

ダイナミック アクセス ポートには、次の制限事項が適用されます。

- ソフトウェアは、Catalyst 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。スイッチは、VMPS サーバではありません。ポートをダイナミックとして設定するには、事前に VMPS サーバを設定する必要があります。
- ダイナミック アクセス ポートは、エンドステーションの接続にだけ使用します。ブリッジングプロトコルを使用するスイッチまたはルータにダイナミック アクセス ポートを接続すると、接続が切断されることがあります。
- STP がダイナミック アクセス ポートを STP ブロッキング ステートにしないように、ネットワークを設定します。ダイナミック アクセス ポートでは、PortFast 機能が自動的にイネーブルになります。
- ダイナミック アクセス ポートは、1 つの VLAN にだけ属することができ、VLAN タギングは使用しません。
- ダイナミック アクセス ポートを次のように設定することはできません。
  - EtherChannel ポート グループのメンバ (ダイナミック アクセス ポートは、他のダイナミック ポートなど、他のポートとはグループ化できません)
  - スタティック アドレス エントリ内の送信元または宛先ポート
  - モニタ ポート

#### 例

次の例では、アクセス モードで動作するスイッチド ポート インターフェイスが、デフォルト VLAN ではなく VLAN 2 で動作するように変更します。

```
Switch(config-if)# switchport access vlan 2
```

設定を確認するには、**show interfaces interface-id switchport** 特権 EXEC コマンドを入力して、Administrative Mode 行および Operational Mode 行の情報を調べます。

#### 関連コマンド

| コマンド                              | 説明  |
|-----------------------------------|---|
| <b>show interfaces switchport</b> | 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。 |
| <b>switchport mode</b>            | ポートの VLAN メンバシップ モードを設定します。                                     |

# switchport autostate exclude

VLAN インターフェイス（スイッチ仮想インターフェイス）のラインステートのアップまたはダウンの計算からインターフェイスを除外するには、**switchport autostate exclude** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**switchport autostate exclude**

**no switchport autostate exclude**



(注)

このコマンドは、スイッチが IP サービス イメージを稼働している場合にだけ使用できます。

## 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

VLAN 上のすべてのポートを VLAN インターフェイス リンクアップ計算に含めます。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

SVI に属するレイヤ 2 アクセス ポートまたはトランク ポートで **switchport autostate exclude** コマンドを入力します。

ポートが関連 VLAN のトラフィックを転送している場合、VLAN インターフェイス（SVI）は起動しています。VLAN 上のすべてのポートがダウンしているかブロックしている場合、SVI はダウンしています。SVI ライン ステートを起動するには、VLAN 上の少なくとも 1 つのポートを起動して、転送させる必要があります。**switchport autostate exclude** コマンドを使用すると、SVI インターフェイスのラインステート アップまたはダウン計算からポートを除外できます。たとえば、モニタリング ポートがアクティブなだけで VLAN が起動していると思なされないようにするために、計算からモニタリング ポートを除外できます。

ポートで **switchport autostate exclude** コマンドを入力すると、このコマンドはポートでイネーブルになっているすべての VLAN に適用されます。

インターフェイスの autostate モードを確認するには、**show interface interface-id switchport** 特権 EXEC コマンドを入力します。モードが設定されていないと、autostate モードが表示されません。

## 例

次の例では、インターフェイスで autostate 除外を設定して、設定を確認する方法を示します。

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# switchport autostate exclude
Switch(config-if)# end
Switch# show interface gigabitethernet1/1 switchport
Name: Gi1/1
Switchport: Enabled
Administrative Mode: dynamic auto
```

```
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative host-association: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Autostate mode exclude
```

**関連コマンド**

| コマンド  | 説明  |
|---|---|
| <b>show interfaces</b><br>[ <i>interface-id</i> ] <b>switchport</b> | autostate モード（設定されている場合）を含む、スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示します。                         |
| <b>show running-config</b>  | 現在の動作設定を表示します。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# switchport backup interface

Flex Link を設定するには、相互にバックアップするインターフェイスのペアは、レイヤ 2 インターフェイスで **switchport backup interface** インターフェイス コンフィギュレーション コマンドを使用します。Flex Link 設定を削除するには、このコマンドの **no** 形式を使用します。

```
switchport backup interface [FastEthernet interface-id | GigabitEthernet interface-id |
Port-channel interface-id | TenGigabitEthernet interface-id ] {mmu primary vlan
interface-id | multicast fast-convergence | preemption {delay delay-time | mode} | prefer vlan
vlan-id}
```

```
no switchport backup interface [FastEthernet interface-id | GigabitEthernet interface-id |
Port-channel interface-id | TenGigabitEthernet interface-id ] {mmu | multicast
fast-convergence | preemption {delay delay-time | mode} | prefer vlan vlan-id}
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|  |   |
|--|---|
| <b>FastEthernet</b>                            | (任意) ファスト イーサネット IEEE 802.3 のポート名を指定します。指定できる範囲は 0 ~ 9 です。  |
| <b>GigabitEthernet</b>                         | (任意) ギガビット イーサネット IEEE 802.3z ポート名を指定します。指定できる範囲は 0 ~ 9 です。   |
| <b>Port-channel</b>                            | (任意) インターフェイスのイーサネット チャネルを指定します。指定できる範囲は 0 ~ 48 です。   |
| <b>TenGigabitEthernet</b>                      | (任意) 10 ギガビット イーサネット ポート名を指定します。指定できる範囲は 0 ~ 9 です。  |
| <i>interface-id</i>                            | 設定されるインターフェイスのバックアップ リンクとして動作するレイヤ 2 インターフェイスは、このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポートチャネル範囲は 1 ~ 48 です。 |
| <b>mmu primary</b><br><b>vlan interface-id</b> | バックアップ インターフェイス ペアの MAC 移動更新 (MMU) を設定します。  |
| <b>multicast</b><br><b>fast-convergence</b>    | マルチキャスト高速コンバージェンス パラメータを指定します。  |
| <b>preemption</b>                              | バックアップ インターフェイス ペアの切り替えスキームを設定します。  |
| <b>delay delay-time</b>                        | プリエンプション遅延を指定します。有効な値は 1 ~ 300 秒です。   |
| <b>mode</b>                                    | プリエンプションモードを <b>bandwidth</b> 、 <b>forced</b> 、または <b>off</b> に設定します。   |
| <b>prefer vlan vlan-id</b>                     | 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。                                   |
| <b>off</b>                                     | バックアップからアクティブへのプリエンプションが発生しないことを指定します。  |
| <b>delay delay-time</b>                        | プリエンプション遅延を指定します。有効な値は 1 ~ 300 秒です。   |

## デフォルト

デフォルトは、Flex Link が定義されていません。プリエンプション モードはオフです。プリエンプションを行いません。プリエンプション遅延は 35 秒に設定されています。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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。この機能はスパニングツリー プロトコル (STP) の代わりに提供され、ユーザが STP をオフにしても基本的なリンク冗長性を維持できます。

- このコマンドは、レイヤ 2 インターフェイスに対してだけ使用可能です。
- 任意のアクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスがバックアップ リンクになるのは、1 つのアクティブ リンクに対してだけです。アクティブ リンクは別の Flex Link ペアに属することはできません。
- バックアップ リンクはアクティブ リンクと同じタイプ (たとえばファスト イーサネットやギガビット イーサネット) でなくてもかまいません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の Flex Link を同様の特性で設定する必要があります。
- いずれのリンクも EtherChannel に属するポートにはなれません。ただし、2 つのポート チャネル (EtherChannel 論理インターフェイス) を Flex Link として設定できます。また、ポート チャネルか物理インターフェイスのいずれか一方をアクティブ リンクにして、ポート チャネルと物理インターフェイスポートを Flex Link として設定できます。
- STP がスイッチに設定されている場合、Flex Link はすべての有効な VLAN で STP に参加しません。STP が動作していない場合、設定されているトポロジでループが発生していないことを確認してください。

## 例

次の例では、2つのインターフェイスを Flex Link として設定する例を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/1
Switch(conf-if)# switchport backup interface fastethernet1/2
Switch(conf-if)# end
```

次の例では、常にバックアップのプリエンブションを行うようファスト イーサネット インターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/1
Switch(conf-if)# switchport backup interface fastethernet1/2 preemption forced
Switch(conf-if)# end
```

次の例では、ファスト イーサネット インターフェイスのプリエンブション遅延時間を設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/1
Switch(conf-if)# switchport backup interface fastethernet1/2 preemption delay 150
Switch(conf-if)# end
```

## switchport backup interface

次の例では、MMU プライマリ VLAN としてファストイーサネットインターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/1
Switch(conf-if)# switchport backup interface fastethernet1/2 mmu primary vlan 1021
Switch(conf-if)# end
```

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

次の例では、優先 VLAN の設定方法を示します。

```
Switch(config)# interface gigabitEthernet 1/2
Switch(config-if)# switchport backup interface gigabitEthernet 1/1 prefer vlan 60,100-120
```

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

この例では、VLAN 60 および 100 ~ 120 がスイッチに設定されています。

```
Switch(config)# interface gigabitEthernet 1/2
Switch(config-if)# switchport backup interface gigabitEthernet 1/1 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合は、Gi1/2 が VLAN 1 ~ 50 のトラフィックを転送し、Gi1/1 が VLAN 60 および 100 ~ 120 のトラフィックを転送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

| Active Interface   | Backup Interface   | State               |
|--------------------|--------------------|---------------------|
| GigabitEthernet1/2 | GigabitEthernet1/1 | Active Up/Backup Up |

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると (LINK\_DOWN)、このインターフェイスで優先される VLAN は、Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gi1/2 がダウンすると、Gi1/1 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                 |
|--------------------|--------------------|-----------------------|
| GigabitEthernet1/2 | GigabitEthernet1/1 | Active Down/Backup Up |

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gi1/2 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 Gi1/1 でブロックされ、Gi1/2 に転送されます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

| Active Interface   | Backup Interface   | State               |
|--------------------|--------------------|---------------------|
| GigabitEthernet1/2 | GigabitEthernet1/1 | Active Up/Backup Up |

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

次の例では、インターフェイス Gi1/1 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 1/1
Switch(config-if)# switchport backup interface gigabitEthernet 1/2 multicast
fast-convergence
Switch(config-if)# end
```

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

```
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface      Backup Interface      State
-----
GigabitEthernet1/1  GigabitEthernet1/2  Active Up/Backup Standby
  Preemption Mode    : off
  Multicast Fast Convergence : On
  Bandwidth : 1000000 Kbit (Gi1/1), 1000000 Kbit (Gi1/2)
  Mac Address Move Update Vlan : auto
```

#### 関連コマンド

| コマンド   | 説明  |
|--|---|
| <b>show interfaces</b> [ <i>interface-id</i> ]<br><b>switchport backup</b> | 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

不明のマルチキャストまたはユニキャスト 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

|                  |  |
|------------------|--|
| <b>multicast</b> | 不明のマルチキャスト トラフィックがブロックされるように指定します。<br><b>(注)</b> 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せん。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。 |
| <b>unicast</b>   | 不明のユニキャスト トラフィックがブロックされるように指定します。  |

## 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 |
|------|------|

## 使用上のガイドライン

デフォルトでは、不明な MAC アドレスを持つすべてのトラフィックがすべてのポートに送信されます。保護ポートまたは非保護ポート上の不明なマルチキャストまたはユニキャスト トラフィックをブロックすることができます。不明なマルチキャストまたはユニキャスト トラフィックが保護ポートでブロックされない場合、セキュリティに問題のある場合があります。

マルチキャスト トラフィックでは、ポートブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

不明なマルチキャストまたはユニキャスト トラフィックのブロックは、保護ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。

パケットのブロックに関する情報は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

## 例

次の例では、インターフェイス上で不明なユニキャスト トラフィックをブロックする方法を示します。

```
Switch(config-if)# switchport block unicast
```

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

## 関連コマンド

| コマンド                              | 説明  |
|-----------------------------------|---|
| <b>show interfaces switchport</b> | 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

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            |
|-----------|-----------------|
| 15.0(1)EY | 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   |
|-----------------------------------|--|
| <b>show interfaces switchport</b> | スイッチポート モードを含む、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 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。モードをデバイスの適切なデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

```
switchport mode {access | dot1q-tunnel | dynamic {auto | desirable} | trunk}
```

```
no switchport mode {access | dot1q-tunnel | dynamic | trunk}
```

## 構文の説明

|                          |  |
|--------------------------|--|
| <b>access</b>            | ポートをアクセス モード ( <b>switchport access vlan</b> 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) に設定します。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。 |
| <b>dynamic auto</b>      | インターフェイス トランキング モード ダイナミック パラメータを <b>auto</b> に設定して、インターフェイスがリンクをトランク リンクに変換するように指定します。これがデフォルトのスイッチ ポート モードになります。   |
| <b>dynamic desirable</b> | インターフェイス トランキング モード ダイナミック パラメータを <b>desirable</b> に設定して、インターフェイスがリンクをトランク リンクにアクティブに変換するように指定します。   |
| <b>trunk</b>             | トランクにポートを無条件に設定します。ポートは VLAN レイヤ 2 インターフェイスをトランキングします。ポートは、送信元の VLAN を識別するカプセル化 (タグ付き) フレームを送受信します。トランクは、2 つのスイッチ間、またはスイッチとルータ間のポイントツーポイントリンクです。   |

## デフォルト

デフォルト モードは **dynamic auto** です。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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キング モードになり、接続先のインターフェイスがリンクからトランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

**dynamic auto** モードを入力した場合に、近接インターフェイスが **trunk** または **desirable** モードに設定されると、インターフェイスはリンクをトランク リンクに変換します。

**dynamic desirable** モードを入力した場合に、近接インターフェイスが **trunk**、**desirable**、または **auto** モードに設定されると、インターフェイスはトランク インターフェイスになります。

トランキングを自動ネゴシエーションするには、インターフェイスが同じ VLAN トランキング プロトコル (VTP) ドメインに存在する必要があります。トランク ネゴシエーションは、ポイントツーポイント プロトコルであるダイナミック トランキング プロトコル (DTP) によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。この事態を避けるには、DTP をサポートしない装置に接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていない装置でトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

**dot1q-tunnel** を入力すると、ポートは IEEE 802.1X 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。

IEEE 802.1x 機能は、次の方法でスイッチ ポート モードに作用します。

- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ポート設定で IEEE 802.1x を **dynamic auto** または **dynamic desirable** にイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードを **dynamic auto** または **dynamic desirable** に変更しようとしても、ポート モードは変更されません。
- ダイナミック アクセス (VLAN Query Protocol (VQP)) ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを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。

## 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 gigabitethernet1/1
Switch(config-if)# switchport mode access
```

次の例では、ポートを **dynamic desirable** モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode dynamic desirable
```

次の例では、ポートをトランク モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode trunk
```

## ■ switchport mode

## 関連コマンド

| コマンド                                       | 説明   |
|--|--|
| <a href="#">show interfaces switchport</a> | 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。 |
| <a href="#">switchport access</a>          | 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。                   |
| <a href="#">switchport trunk</a>           | 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 nonegotiate

ダイナミック トランキング プロトコル (DTP) ネゴシエーション パケットがレイヤ 2 インターフェイスで送信されないように指定するには、**switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用します。スイッチは、このインターフェイス上で DTP ネゴシエーションを行いません。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**switchport nonegotiate**

**no switchport nonegotiate**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デフォルトでは、トランキング ステータスを学習するために、DTP ネゴシエーションを使用します。

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**nonegotiate** ステータスを解除するには、**switchport nonegotiate** コマンドの **no** 形式を使用します。

このコマンドが有効なのは、インターフェイス スイッチ ポート モードがアクセスまたはトランク (**switchport mode access** または **switchport mode trunk** インターフェイス コンフィギュレーション コマンドで設定) の場合だけです。**dynamic** (**auto** または **desirable**) モードでこのコマンドを実行しようとすると、エラーが返されます。

DTP をサポートしないインターネットワーキング デバイスでは、DTP フレームが正しく転送されず、設定に矛盾が生じることがあります。この問題を回避するには、**switchport nonegotiate** コマンドを使用して DTP をオフにし、DTP をサポートしていないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定します。

**switchport nonegotiate** コマンドを入力した場合、このインターフェイスでは DTP ネゴシエーション パケットが送信されません。デバイスがトランキングを実行するかどうかは、**mode** パラメータ (**access** または **trunk**) によって決まります。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスでのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

## 例

次の例では、ポートに対してトランキング モードのネゴシエートを制限し、(モードの設定に応じて) トランク ポートまたはアクセス ポートとして動作させる方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport nonegotiate
```

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

## ■ switchport nonegotiate

## 関連コマンド

| コマンド                                       | 説明   |
|--|--|
| <a href="#">show interfaces switchport</a> | 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。 |
| <a href="#">switchport mode</a>            | ポートの VLAN メンバーシップ モードを設定します。                             |

# switchport port-security

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には、キーワードを指定せずに **switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。キーワードを指定すると、セキュア MAC アドレス、スティッキ MAC アドレス ラーニング、セキュア MAC アドレスの最大数、または違反モードが設定されます。ポートセキュリティをディセーブルにしたり、またはパラメータをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

```
switchport port-security [mac-address mac-address [vlan {vlan-id} | {access | voice}]] |
  mac-address sticky [mac-address | vlan {vlan-id} | {access | voice}]] [maximum value [vlan
  {vlan-list} | {access | voice}]]]
```

```
no switchport port-security [mac-address mac-address [vlan {vlan-id} | {access | voice}]] |
  mac-address sticky [mac-address | vlan {vlan-id} | {access | voice}]] [maximum value [vlan
  {vlan-list} | {access | voice}]]]
```

```
switchport port-security [aging] [violation {protect | restrict | shutdown | shutdown vlan}]
```

```
no switchport port-security [aging] [violation {protect | restrict | shutdown | shutdown vlan}]
```

## 構文の説明

|                                       |   |
|---------------------------------------|---|
| <b>mac-address mac-address</b>        | (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。   |
| <b>vlan vlan-id</b>                   | (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。  |
| <b>vlan access</b>                    | (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。  |
| <b>vlan voice</b>                     | (任意) アクセス ポートでだけ、VLAN を音声 VLAN として指定します。<br><br><b>(注)</b> <b>voice</b> キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合に限り利用可能です。  |
| <b>mac-address sticky mac-address</b> | (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、 <b>mac-address sticky</b> 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。<br><br>(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。   |
| <b>maximum value</b>                  | (任意) インターフェイスの最大セキュア MAC アドレス数を設定します。スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management (SDM) テンプレートによって決められます。詳細は、 <a href="#">sdm prefer</a> グローバル コンフィギュレーション コマンドを参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。<br><br>デフォルトの設定は 1 です。 |

|                              |  |
|------------------------------|--|
| <b>vlan</b> <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します。 <b>vlan</b> 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"> <li>• <b>vlan</b> : VLAN ごとに最大値を設定します。</li> <li>• <b>vlan</b> <i>vlan-list</i> : 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。</li> </ul>                                      |
| <b>aging</b>                 | (任意) <b>switchport port-security aging</b> コマンドを参照してください。  |
| <b>violation</b>             | (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 <b>shutdown</b> です。   |
| <b>protect</b>               | 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 ポートに保護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>   |
| <b>restrict</b>              | 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。   |
| <b>shutdown</b>              | 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 <b>errdisable</b> 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 <b>errdisable</b> ステートの場合、 <b>errdisable recovery cause psecure-violation</b> 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、 <b>shutdown</b> および <b>no shutdown</b> 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。 |
| <b>shutdown vlan</b>         | VLAN 単位のシャットダウンにセキュリティ違反モードを設定します。このモードでは、違反が発生した VLAN だけが <b>errdisable</b> になります。  |

## デフォルト

デフォルトでは、ポート セキュリティはディセーブルです。

ポート セキュリティをイネーブルにしてキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数は 1 です。

デフォルトの違反モードは、**shutdown** です。

スティッキ ラーニングはディセーブルです。

コマンドモード インターフェイス コンフィギュレーション

#### コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

#### 使用上のガイドライン

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートには設定できません。
- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ (SPAN) の宛先ポートにすることはできません。
- セキュア ポートを Fast EtherChannel または Gigabit EtherChannel ポート グループに含めることはできません。
- 音声 VLAN では、スタティック セキュアまたはスティッキ セキュア MAC アドレスを設定できません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。
- 音声 VLAN はアクセス ポート上でだけサポートされます。トランク ポート上ではサポートされません。
- インターフェイスのセキュア アドレスの最大値を入力する場合、新しい値が前回の値より大きいと、新しい値によって前回の設定値が上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングをサポートしていません。

セキュア MAC アドレスの最大値がアドレス テーブルに存在し、アドレス テーブルに存在しない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、または別のセキュア ポートのセキュア MAC アドレスとして設定された MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合に、セキュリティ違反が起こります。

セキュア ポートが `errdisable` ステートの場合は、`errdisable recovery cause psecure-violation` グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

インターフェイスのセキュアアドレスの最大値を入力すると、次の事象が発生します。

- 新しい値が前回の値より大きい場合、新しい値によって前回の設定値が上書きされます。
- 新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

スティッキ セキュア MAC アドレスには、次の特性があります。

- **switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス上でスティッキ ラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミック セキュア MAC アドレスを（スティッキ ラーニングがイネーブルになる前にダイナミックに学習されたアドレスも含め）、スティッキ セキュア MAC アドレスに変換し、すべてのスティッキ セキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキ ラーニングをディセーブルする場合、または実行コンフィギュレーションを削除する場合は、スティッキ セキュア MAC アドレスは実行コンフィギュレーションの一部に残りますが、アドレス テーブルからは削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミック アドレスとしてアドレス テーブルに追加されます。
- **switchport port-security mac-address sticky mac-address** インターフェイス コンフィギュレーション コマンドを使用して、スティッキ セキュア MAC アドレスを設定する場合、アドレスはアドレス テーブルと実行コンフィギュレーションに追加されます。ポート セキュリティがディセーブルの場合、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキ セキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくて済みます。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
```

次の例では、違反が発生した場合に VLAN だけをシャットダウンするようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet 0/2  
Switch(config)# switchport port-security violation shutdown vlan
```

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

#### 関連コマンド

| コマンド   | 説明   |
|--|--|
| <b>clear port-security</b>                       | 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。 |
| <b>show port-security address</b>                | 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。   |
| <b>show port-security interface interface-id</b> | 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 タイムと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

|                         |  |
|-------------------------|--|
| <b>static</b>           | 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。   |
| <b>time <i>time</i></b> | 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。 <b>time</b> 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。       |
| <b>type</b>             | エージング タイプを設定します。   |
| <b>absolute</b>         | 絶対エージング タイプを設定します。このポートのすべてのセキュア アドレスは、指定された時間 (分) が経過した後に期限切れとなり、セキュア アドレス リストから削除されます。     |
| <b>inactivity</b>       | 非アクティビティ エージング タイプを設定します。指定された時間内にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュア アドレスが期限切れになります。 |

## デフォルト

ポート セキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。

デフォルトのエージング タイプは **absolute** です。

デフォルトのスタティック エージング動作はディセーブルです。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

特定のポートのセキュア アドレス エージングをイネーブルにするには、ポート エージング タイムを 0 以外の値に設定します。

特定のセキュア アドレスに時間を限定してアクセスできるようにするには、エージング タイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュア アドレスが削除されます。

継続的にアクセスできるセキュア アドレス数を制限するには、エージング タイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュア アドレスが削除され、他のアドレスがセキュアになることができます。

セキュア アドレスへのアクセス制限を解除するには、セキュア アドレスとして設定し、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用して、静的に設定されたセキュア アドレスのエージングをディセーブルにします。

## 例

次の例では、ポートのすべてのセキュア アドレスに対して、エージング タイプを `absolute`、エージング タイムを 2 時間に設定します。

```
Switch(config)# interface 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 タイプを `inactivity`、エージング タイムを 2 分に設定します。

```
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  |
|---------------------------------------|---|
| <code>show port-security</code>       | 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。  |
| <code>switchport port-security</code> | ポート上でポート セキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC アドレスを設定します。 |

# switchport priority extend

着信タグなしフレームのポート プライオリティや、指定のポートに接続された IP Phone が受信するフレームのプライオリティを設定するには、**switchport priority extend** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport priority extend {cos value | trust}
```

```
no switchport priority extend
```

## 構文の説明

|                  |   |
|------------------|---|
| <b>cos value</b> | PC または指定した Class of Service (CoS) 値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は 0 ~ 7 です。7 が最も高いプライオリティです。デフォルトは 0 です。 |
| <b>trust</b>     | PC または接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。   |

## デフォルト

ポートで受信したタグなしフレームには、デフォルト ポート プライオリティは、CoS 値 0 で設定されています。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

音声 VLAN をイネーブルにした場合、スイッチを設定して、Cisco Discovery Protocol (CDP) パケットを送信し、Cisco IP Phone のアクセス ポートに接続される装置からデータ パケットを送信する方法を IP Phone に指示できます。Cisco IP Phone に設定を送信するには、Cisco IP Phone に接続しているスイッチ ポートの CDP をイネーブルにする必要があります (デフォルトでは、CDP はすべてのスイッチ インターフェイスでグローバルにイネーブルです)。

スイッチ アクセス ポート上で音声 VLAN を設定する必要があります。音声 VLAN は、レイヤ 2 ポート上にだけ設定できます。

音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチの Quality of Service (QoS) をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力して、信頼するようにポート信頼状態を設定することを推奨します。

## 例

次の例では、受信した IEEE 802.1p プライオリティを信頼するように、指定されたポートに接続された IP Phone を設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport priority extend trust
```

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

## 関連コマンド

| コマンド   | 説明  |
|--|---|
| <code>show interfaces</code>   | 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>switchport voice vlan {vlan-id   dot1p   none   untagged}</code> | ポートに音声 VLAN を設定します。                         |

# 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、ブロードキャストトラフィックを分離するには、**switchport protected** インターフェイス コンフィギュレーション コマンドを使用します。ポートで保護をディセーブルにするには、このコマンドの **no** 形式を使用します。

**switchport protected**

**no switchport protected**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

保護ポートは定義されていません。すべてのポートが保護されていません。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 gigabitethernet01/2
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。

## 関連コマンド

| コマンド                              | 説明   |
|-----------------------------------|--|
| <b>show interfaces switchport</b> | 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。 |
| <b>switchport block</b>           | 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 | pruning vlan vlan-list}
```

```
no switchport trunk {allowed vlan | native vlan | {pruning vlan}}
```

## 構文の説明

|                               |   |
|-------------------------------|---|
| <b>allowed vlan vlan-list</b> | 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。 <b>none</b> キーワードは無効です。デフォルトは <b>all</b> です。 |
| <b>native vlan vlan-id</b>    | インターフェイスがトランキング 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。  |
| <b>pruning vlan vlan-list</b> | トランキング モードの場合に、VTP プルーニングに適格な VLAN のリストを設定します。 <b>all</b> キーワードは無効です。   |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

*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** は空のリストを示します。特定の VLAN を設定するか、または少なくとも 1 つの VLAN を設定する必要があるコマンドでは、このキーワードを使用できません。
- **add** は現在設定されている VLAN リストを置き換えないで、定義済み VLAN リストを追加します。有効な ID は 1 ~ 1005 です。場合によっては、拡張範囲 VLAN (VLAN ID が 1005 より上) を使用できます。



**(注)** 許可 VLAN リストに拡張範囲 VLAN を追加できますが、プルーニング適格 VLAN リストには追加できません。

カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。

- **remove** は現在設定されている VLAN リストを置き換えないで、リストから定義済み VLAN リストを削除します。有効な ID は 1 ~ 1005 です。場合によっては、拡張範囲 VLAN ID を使用できます。



(注) 許可 VLAN リストから拡張範囲 VLAN を削除できますが、プルーニング適格リストからは削除できません。

カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。

- **except** は定義済み VLAN リスト以外の、計算する必要がある VLAN を示します (指定した VLAN を除く VLAN が追加されます)。有効な ID は 1 ~ 1005 です。カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。
- **vlan-atom** は、1 ~ 4094 内の単一の VLAN 番号、または 2 つの VLAN 番号で指定された連続した範囲の VLAN で、小さい方の値を先頭にハイフンで区切ります。

ネイティブ VLAN :

- 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)、ポート集約プロトコル (PAgP)、Link Aggregation Control Protocol (LACP)、ダイナミック トランッキング プロトコル (DTP)、および VLAN 1 の VLAN トランッキング プロトコル (VTP)) を送受信し続けます。
- **allowed vlan** コマンドの **no** 形式は、リストをデフォルト リスト (すべての VLAN を許可) にリセットします。

トランク プルーニング :

- プルーニング適格リストは、トランク ポートだけに適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLAN をプルーニングしない場合は、プルーニング適格リストから VLAN を削除します。プルーニング不適格の VLAN は、フラッドイング トラフィックを受信します。
- VLAN 1、VLAN 1002 ~ 1005、および拡張範囲 VLAN (VLAN 1006 ~ 4094) は、プルーニングできません。

## 例

次の例では、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
```

次の例では、プルーン適格リストから VLAN 3 および 10 ~ 15 を削除する方法を示します。

```
Switch(config)# interface gigabitethernet0/2  
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

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

#### 関連コマンド

| コマンド                              | 説明  |
|-----------------------------------|---|
| <b>show interfaces switchport</b> | 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。 |
| <b>switchport mode</b>            | ポートの VLAN メンバーシップ モードを設定します。                                    |

# switchport voice vlan

ポートに音声 VLAN 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。**switchport voice vlan** インターフェイス コンフィギュレーション コマンドを使用します。

```
switchport voice vlan {vlan-id | dot1p | none | untagged}
```

```
no switchport voice vlan
```

## 構文の説明

|                 |   |
|-----------------|---|
| <b>vlan-id</b>  | 音声トラフィックに使用する VLAN を設定します。指定できる範囲は 1 ~ 4094 です。デフォルトでは、IP Phone はプライオリティ 5 を使用して音声トラフィックを転送します。                                       |
| <b>dot1p</b>    | IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように電話機を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。 |
| <b>none</b>     | 音声 VLAN に関して IP Phone に指示しません。IP Phone のキーパッドから入力された設定を使用します。   |
| <b>untagged</b> | タグなしの音声トラフィックを送信するように電話機を設定します。これが IP Phone のデフォルト設定になります。  |

## デフォルト

デフォルトでは、スイッチは IP Phone を自動設定しません (**none**)。

デフォルトでは、IP Phone はフレームにタグを付けません。

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

レイヤ 2 アクセスポート上で音声 VLAN を設定する必要があります。

スイッチの Cisco IP Phone に接続しているスイッチポート上の Cisco Discovery Protocol (CDP) をイネーブルにし、IP フォンに設定情報を送信する必要があります。デフォルトでは、CDP はインターフェイス上でグローバルにイネーブルです。

音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチの Quality of Service (QoS) をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力して、信頼するようにポート信頼状態を設定することを推奨します。

VLAN ID を入力すると、IP Phone は IEEE 802.1X フレームの音声トラフィックを指定された VLAN ID タグ付きで転送します。スイッチは IEEE 802.1X 音声トラフィックを音声 VLAN に入れます。

**dot1p**、**none**、または **untagged** を選択した場合、スイッチは指定の音声トラフィックをアクセス VLAN に入れます。

すべての設定で、音声トラフィックはレイヤ 2 の IP precedence 値を運びます。音声トラフィックのデフォルトは 5 です。

音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。

アクセス VLAN で任意のポート セキュリティ タイプがイネーブルにされた場合、音声 VLAN でダイナミック ポート セキュリティは自動的にイネーブルになります。

音声 VLAN では、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

**例**

次の例では、VLAN 2 をポート用音声 VLAN として設定します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport voice vlan 2
```

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

**関連コマンド**

| コマンド   | 説明   |
|--|--|
| <b>show interfaces interface-id switchport</b> | 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。                |
| <b>switchport priority extend</b>              | 指定されたポートに接続されたデバイスが、着信ポートで受信したプライオリティ トラフィックを処理する方法を指定します。 |

# sync flash sdflash

宛先のフラッシュ システムにフラッシュ イメージをコピーするには、EXEC モードの **sync flash sdflash** コマンドを使用します。このコマンドは、環境変数 **BOOT** ファイルをコピー先のフラッシュ環境変数にコピーします。このとき、コピー元のフラッシュ名はコピー先のフラッシュ名に置き換えられます。

```
sync flash sdflash {ios-image-name | skip | save-old-files}
```

## 構文の説明

|                       |   |
|-----------------------|---|
| <i>ios-image-name</i> | 同期する Cisco IOS イメージ。これは、イメージ名またはフルパス名にすることができます。さらに、Cisco IOS イメージ名は宛先のフラッシュの <b>BOOT</b> 変数にコピーされます。 |
| <b>skip</b>           | config.text、Cisco IOS イメージ、vlan.dat* のいずれか 1 つまたはすべてのファイルのコピーをスキップするよう指定します。                          |
| <b>save-old-files</b> | Cisco IOS ファイルを保存します。   |

## デフォルト

ファイルは保存されません。

Cisco IOS イメージ名が指定されていない場合、Cisco IOS イメージはコピー元のフラッシュ **BOOT** 環境変数からコピー先のフラッシュにコピーされます。

**skip** キーワードが指定されない場合、すべてのファイルがコピーされます。

## コマンドモード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 IOS イメージ名が同じ場合、保存されているイメージ名でこのイメージ名も保存されます。コピー元とコピー先のパスが同じディレクトリ名を持つ場合、コピー先のディレクトリは **\*-saved** として保存されます。保存されたディレクトリのすべてのファイルは同じままです。同じ名前の新しいディレクトリは同期操作によってコピー先のフラッシュ上に作成されます。

## 例

次の例では、SD フラッシュからオンボード フラッシュに Cisco IOS イメージを同期する方法を示します。

```
Switch # sync sdflash: flash: standard_config new_config skip config.txt vlan.dat
```

# system mtu

最大パケット サイズまたは最大伝送単位 (MTU) サイズをギガビット イーサネット ポート、ルーテッドポート、またはファストイーサネット (10/100) ポートに設定するには、**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 Mb/s 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>   | 1000 Mb/s 以上で稼働しているギガビット イーサネット ポートのシステム ジャンボ MTU を設定します。指定できる範囲は 1500 ~ 9000 バイトです。これは、ギガビット イーサネット ポートの物理ポートで受信する最大 MTU です。  |
| <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            |
|-----------|-----------------|
| 15.0(1)EY | 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。

システム MTU 設定は、NVRAM のスイッチ環境変数に保存され、スイッチをリロードするときに有効になります。システム MTU のルーティング設定とは異なり、**system mtu** および **system mtu jumbo** コマンドを使用して入力する MTU 設定は、**copy running-config startup-config** 特権 EXEC コマンドを入力しても、スイッチの Cisco 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 で稼働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 packets (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 で稼働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 で稼働するインターフェイスで受信できませんが、宛先インターフェイスが 10 または 100 Mbps で稼働している場合、パケットはドロップされます。

## 例

次の例では、1000 Mbps 以上で稼働しているギガビット イーサネット ポートの最大ジャンボ パケット サイズを 1800 バイトに設定する方法を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

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

## 関連コマンド

| コマンド                            | 説明   |
|---------------------------------|--|
| <a href="#">show system mtu</a> | ファスト イーサネット ポート、ギガビット イーサネット ポート、およびルーテッド ポートに設定されたパケット サイズを表示します。 |

# test cable-diagnostics tdr

インターフェイス上でタイム ドメイン反射率計 (TDR) 機能を実行するには、特権 EXEC モードで **test cable-diagnostics tdr** コマンドを使用します。

**test cable-diagnostics tdr interface interface-id**

|          |                               |                          |
|----------|-------------------------------|--------------------------|
| 構文の説明    | <b>interface interface-id</b> | 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    | 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                     |
|          | 15.0(1)EY                     | このコマンドが追加されました。          |

## 使用上のガイドライン

TDR は、銅線のイーサネット 10/100 および 10/100/1000 ポートでサポートされます。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 Gi0/3 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.
```

## 関連コマンド

| コマンド                                       | 説明             |
|--|----------------|
| <a href="#">show cable-diagnostics tdr</a> | TDR 結果が表示されます。 |

# test relay

リレー回路をオンまたはオフにするには、特権 EXEC モードで **test relay** コマンドを使用します。

**test relay {major | minor} {on| off}**



## 注意

**test** コマンドを使用するとリレーのステート（オンまたはオフ）が変更されます。変更前のステートは保存されません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

アラート デバイスへのリレー回路接続を確認するには、**test relay** 特権 EXEC コマンドを使用します。アラーム条件を作成せずにアラーム スキャナをテストできます。

## 例

次の例では、メジャー リレー回路をオンにする方法を示します。

```
Switch# test relay major on
```

## 関連コマンド

| コマンド                                | 説明   |
|-------------------------------------|--|
| <a href="#">show alarm profile</a>  | 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。 |
| <a href="#">show alarm settings</a> | 環境アラーム設定およびオプションが表示されます。   |

# 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 アドレスまでを通過するパケットのレイヤ 2 パスを表示するには、特権 EXEC モードで **traceroute mac** コマンドを使用します。

```
traceroute mac [interface interface-id] {source-mac-address} [interface interface-id]
               {destination-mac-address} [vlan vlan-id] [detail]
```

| 構文の説明                          |  |
|--------------------------------|--|
| <b>interface interface-id</b>  | (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。   |
| <b>source-mac-address</b>      | 送信元スイッチの MAC アドレスを指定します (16 進数)。   |
| <b>destination-mac-address</b> | 宛先スイッチの MAC アドレスを指定します (16 進数)。  |
| <b>vlan vlan-id</b>            | (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。 |
| <b>detail</b>                  | (任意) 詳細情報を表示するように指定します。  |

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            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

レイヤ 2 の **traceroute** を適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークのすべてのスイッチでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

スイッチがレイヤ 2 パス内でレイヤ 2 **traceroute** をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 **trace** クエリーを送信し続け、タイムアウトにします。

パス内で識別可能なホップ 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 **traceroute** 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

## 例

次の例では、送信元および宛先 MAC アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# tracert mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[switch_mmmodel] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5          (2.2.5.5      ) :   Gi0/3 => Gi0/1
con1          (2.2.1.1      ) :   Gi0/1 => Gi0/2
con2          (2.2.2.2      ) :   Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**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 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[switch_mmmodel] (2.2.6.6)
con6 /switch_mmmodel/ 2.2.6.6 :
      Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / switch_mmmodel / 2.2.5.5 :
      Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / switch_mmmodel / 2.2.1.1 :
      Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 /switch_mmmodel / 2.2.2.2 :
      Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先スイッチのインターフェイスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# tracert mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[switch_mmmodel] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5          (2.2.5.5      ) :   Gi0/3 => Gi0/1
con1          (2.2.1.1      ) :   Gi0/1 => G0/2
con2          (2.2.2.2      ) :   Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、スイッチが送信元スイッチに接続されていない場合のレイヤ 2 のパスを示します。

```
Switch# tracert mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[switch_mmmodel] (2.2.5.5)
con5 / switch_mmmodel / 2.2.5.5 :
      Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / switch_mmmodel / 2.2.1.1 :
      Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / switch_mmmodel / 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  |
|-----------------------------------|---|
| <a href="#">traceroute mac ip</a> | 指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。 |

# traceroute mac ip

指定された送信元 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を通過するパケットのレイヤ 2 パスを表示するには、特権 EXEC モードで **traceroute mac ip** コマンドを使用します。

```
traceroute mac ip {source-ip-address | source-hostname} {destination-ip-address |
destination-hostname} [detail]
```

## 構文の説明

|                               |  |
|-------------------------------|--|
| <i>source-ip-address</i>      | 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）。 |
| <i>destination-ip-address</i> | 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）。  |
| <i>source-hostname</i>        | 送信元スイッチの IP ホスト名。                              |
| <i>destination-hostname</i>   | 宛先スイッチの IP ホスト名。                               |
| <b>detail</b>                 | （任意）詳細情報を表示するように指定します。                         |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

レイヤ 2 の traceroute を適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークのすべてのスイッチでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

スイッチがレイヤ 2 パス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

パス内で識別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、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定した場合、スイッチはアドレス解決プロトコル (ARP) を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を関連付けます。

- 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
- ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスは同一のサブネットにある必要があります。IP アドレスが解決されないと、パスは識別されず、エラーメッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラーメッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

## 例

次の例では、**detail** キーワードを使用して、送信元および宛先 IP アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / switch_mmodel / 2.2.6.6 :
      Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5 / switch_mmodel / 2.2.5.5 :
      Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / switch_mmodel / 2.2.1.1 :
      Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / switch_mmodel / 2.2.2.2 :
      Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5           (2.2.5.5       ) :   Gi0/3 => Gi0/1
con1           (2.2.1.1       ) :   Gi0/1 => Gi0/2
con2           (2.2.2.2       ) :   Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 のパスを示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>traceroute mac</b> | 指定の送信元 MAC アドレスから、指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示します。 |

# trust

**class** ポリシーマップ コンフィギュレーションまたは **class-map** グローバル コンフィギュレーション コマンドで分類されたトラフィックの信頼状態を定義するには、**trust** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
trust [cos | dscp | ip-precedence]
```

```
no trust [cos | dscp | ip-precedence]
```

## 構文の説明

|                      |   |
|----------------------|---|
| <b>cos</b>           | (任意) パケットの Class of Service (CoS) 値を使用して、入力パケットを分類します。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。   |
| <b>dscp</b>          | (任意) パケットの DiffServ コードポイント (DSCP) 値 (8 ビット サービス タイプ フィールドの上位 6 ビット) を使用して、入力パケットを分類します。パケットがタグ付きの場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットがタグなしの場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。 |
| <b>ip-precedence</b> | (任意) パケット IP-precedence 値 (8 ビット サービスタイプ フィールドの上位 3 ビット) を使用して、入力パケットを分類します。パケットがタグ付きの場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットがタグなしの場合、CoS の DSCP マッピングにポートのデフォルト CoS 値が使用されます。              |

## デフォルト

アクションは信頼されていません。キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** です。

## コマンドモード

ポリシー マップ クラス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

特定のトラフィックの Quality of Service (QoS) の信頼動作を他のトラフィックと区別するために、このコマンドを使用します。たとえば、特定の DSCP 値を持つ着信トラフィックが信頼されます。着信トラフィックの DSCP 値と一致し、信頼するクラス マップを設定できます。

このコマンドで設定された信頼性の値は、**mls qos trust** インターフェイス コンフィギュレーション コマンドで設定された信頼性の値を上書きします。

**trust** コマンドは、同一ポリシー マップ内の **set** ポリシー マップ クラス コンフィギュレーション コマンドと相互に排他的な関係にあります。

**trust cos** を指定した場合、QoS は受信した CoS 値、またはデフォルト ポートの CoS 値および CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。

**trust dscp** を指定した場合、QoS は入力パケットから DSCP 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値を、タグなしの非 IP パケットに対しては、デフォルト ポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されません。

**trust ip-precedence** を指定した場合、QoS は入力パケットおよび IP precedence/DSCP マップから IP precedence 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値を、タグなしの非 IP パケットに対しては、デフォルトポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

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

**例**

次の例では、*class1* で分類されたトラフィックの着信 DSCP 値を信頼するようにポート信頼状態を定義する方法を示します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 2000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

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

**関連コマンド**

| コマンド                   | 説明   |
|------------------------|--|
| <b>class</b>           | 指定されたクラスマップ名のトラフィック分類一致条件 ( <b>police</b> 、 <b>set</b> 、および <b>trust</b> ポリシー マップ クラス コンフィギュレーション コマンドによる) を定義します。 |
| <b>police</b>          | 分類したトラフィックにポリサーを定義します。   |
| <b>policy-map</b>      | 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。  |
| <b>set</b>             | パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。  |
| <b>show policy-map</b> | QoS ポリシー マップを表示します。  |

# udld

単方向リンク検出 (UDLD) 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 タイマーの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

|  |  |
|--|--|
| <b>aggressive</b>                                    | 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。                     |
| <b>enable</b>  | 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。                       |
| <b>message time</b><br><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。範囲は 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            |
|-----------|-----------------|
| 15.0(1)EY | 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になります。時間を減少させると、検出応答を高速にすることができますが、CPU の負荷も高くなります。

このコマンドが作用するのは、光ファイバ インターフェイスだけです。他のインターフェイス タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。

UDLD によ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 コマンドを入力し、UDLD を再びグローバルに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 コマンドを入力し、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  |
|-------------------|---|
| <b>show udld</b>  | 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。  |
| <b>udld port</b>  | 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 <b>udld</b> 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。 |
| <b>udld reset</b> | 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上で単方向リンク検出 (UDLD) をイネーブルにするか、または **udld** グローバル コンフィギュレーション コマンドによって光ファイバインターフェイスがイネーブルにされるのを防ぎます。**udld** グローバル コンフィギュレーション コマンド設定に戻すには、このコマンドの **no** 形式を使用し、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 port [aggressive]**

**no udld port [aggressive]**

## 構文の説明

**aggressive** (任意) 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            |
|-----------|-----------------|
| 15.0(1)EY | 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、このポートは単方向リンクを検出できません。

UDLD は、ノーマル (デフォルト) とアグレッシブの 2 つの動作モードをサポートしています。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単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「Configuring UDLD」の章を参照してください。

UDLD をノーマル モードでイネーブルにするには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。UDLD をアグレッシブ モードでイネーブルにするには、**udld port aggressive** インターフェイス コンフィギュレーション コマンドを使用します。

UDLD の制御を **udld enable** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバポートでディセーブルにしたりする場合は、光ファイバポートで **no udld port** コマンドを使用します。

**udld enable** または **udld aggressive** グローバル コンフィギュレーション コマンドの設定を無効にする場合は、光ファイバポートで **udld port aggressive** コマンドを使用します。この設定を削除して UDLD イネーブル化の制御を **udld** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバポートでディセーブルにしたりする場合は、光ファイバポートで **no** 形式を使用します。

UDLD によってシャットダウンされたインターフェイスをリセットするのに、次のコマンドを使用します。

- **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 コマンドを入力し、UDLD を再びグローバルに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 コマンドを入力し、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   |
|----------------------------|--|
| <b>show running-config</b> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show udld</b>           | 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。   |
| <b>udld</b>                | 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。   |
| <b>udld reset</b>          | 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) によって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、トラフィックが通過を開始するのを再び許可するには (スパンニング ツリー、ポート集約プロトコル (PAgP)、ダイナミック トランッキング プロトコル (DTP) などの他の機能はイネーブルにすると通常の効果を持ちますが)、特権 EXEC モードで **udld reset** コマンドを使用します。

## udld reset

### 構文の説明

このコマンドには、引数またはキーワードはありません。

### 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            |
|-----------|-----------------|
| 15.0(1)EY | 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 の稼働を開始し、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   |
|----------------------------|--|
| <b>show running-config</b> | 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、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show udld</b>           | 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。   |
| <b>udld</b>                | 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。   |
| <b>udld port</b>           | 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 <b>udld</b> 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。       |

# 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、グローバル コンフィギュレーション モードで **vlan** 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。

```
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。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    | なし             |   |
| コマンド モード |                | グローバル コンフィギュレーション   |
| コマンド履歴   | リリース           | 変更箇所  |
|          | 15.0(1)EY      | このコマンドが追加されました。   |

## 使用上のガイドライン

標準範囲 VLAN (VLAN ID 1 ~ 1005) のコンフィギュレーション情報は、常に VLAN データベースに保存されます。VLAN トランッキング プロトコル (VTP) バージョン 3 を使用している場合、または VTP モードがトランスペアレント (VTP バージョン 1 または 2) の場合は、拡張範囲 VLAN (VLAN ID が 1006 以上) を作成することができます。VTP バージョン 3 では、これらの VLAN も VLAN データベースに保存されます。

通常範囲の VLAN (VLAN ID 1 ~ 1005) や拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を追加するには、**vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用します。VTP バージョン 1 およびバージョン 2 を使用する場合は、拡張範囲 VLAN を追加する前に、**vtp transparent** 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を VTP トランスペアレント モードにする必要があります。VTP バージョン 1 および 2 を使用する場合、拡張範囲 VLAN は VTP によって認識されず、VLAN データベースに追加されません。VTP モードがトランスペアレントである場合、VTP モードとドメイン名およびすべての VLAN 設定は実行コンフィギュレーションに保存されますが、この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存することもできます。

VTP バージョン 3 は拡張範囲 VLAN の伝播をサポートしているため、それらを VLAN サーバまたはクライアント モードで作成できます。

VLAN および VTP 設定をスタートアップ コンフィギュレーション ファイルに保存して、スイッチをリブートすると、設定は次のように選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードがトランスペアレントであり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- VTP モードがサーバの場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 個の VLAN の VTP モードおよび VLAN 設定には VLAN データベース情報が使用されます。VTP バージョン 3 では、すべての VLAN ID は VLAN データベース内に存在します。

VTP バージョン 1 およびバージョン 2 では、スイッチが VTP トランスペアレント モードではない場合に拡張範囲 VLAN を作成しようとする、VLAN は拒否され、エラー メッセージが表示されます。

無効な VLAN ID を入力すると、エラー メッセージが表示され、`config-vlan` モードを開始できません。

`vlan` コマンドを VLAN ID を指定して入力すると、`config-vlan` モードがイネーブルになります。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、`config-vlan` 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 コマンドが `config-vlan` 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` と `remote-span` 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。

- **are are-number** : この 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。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ~ 13 です。デフォルトは 7 です。値が入力されない場合、最大数は 0 であると見なされます。
- **backupcrf** : バックアップ CRF モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。
  - この VLAN のバックアップ CRF モードを **enable** (イネーブル) にします。
  - この VLAN のバックアップ CRF モードを **disable** (ディセーブル) にします (デフォルト)。
- **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。FDDI-NET、TrBRF、およびトークンリング NET VLAN については、デフォルトのブリッジ番号は 0 (ソースルーティングブリッジなし) です。type キーワードは、TrCRF VLAN だけに適用され、次のうちのいずれかです。
  - **srb** (ソースルートブリッジ)
  - **srt** (ソースルート トランスペアレント) ブリッジング VLAN
- **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、`config-vlan` モードを終了します。
- **media** : VLAN メディア タイプを定義します。さまざまなメディア タイプで有効なコマンドおよび構文については、表 2-37 を参照してください。



(注) スイッチがサポートするのは、イーサネット ポートだけです。FDDI およびトークンリング メディア固有の特性は、別のスイッチに対する VLAN トランッキング プロトコル (グローバル アドバタイズ) に基づいて設定します。これらの VLAN はローカルに停止されません。

- **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、VTP v2 モードがディセーブルの場合にはトークンリング メディア タイプであり、VTP v2 モードがイネーブルの場合は TrCRF です。
  - **tr-net** は、VTP v2 モードがディセーブルの場合にはトークンリング Network Entity Title (NET) メディア タイプであり、VTP v2 モードがイネーブルの場合は TrBRF メディア タイプです。
- **mtu mtu-size** : 最大伝送単位 (MTU) (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。このパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を定義するときが必要です。指定できる範囲は 0 ~ 1005 です。デフォルトの親 VLAN ID は、FDDI およびトークンリング VLAN では 0 (親 VLAN なし) です。トークンリングおよび TrCRF VLAN の両方で、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。
  - **remote-span** : VLAN をリモート SPAN (RSPAN) 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。VTP がイネーブルの場合、新しい RSPAN VLAN は、1024 より小さい数字の VLAN ID の VTP により伝播されます。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。トークンリング VLAN のデフォルト値は 0 です。FDDI VLAN には、デフォルト設定はありません。
  - **said said-value** : IEEE 802.10 に記載されているセキュリティ アソシエーション ID (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 の 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、**config-vlan** モードを終了したときに有効になります。
  - **state** : VLAN ステータスを指定します。
    - **active** は、VLAN が稼働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** : スパニングツリー エクスプローラ (STE) のホップの最大数を定義します。このキーワードは、TrCRF VLAN だけに適用されます。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。FDDI-NET VLAN の場合、デフォルトの STP タイプは **ieee** です。トークンリング NET VLAN の場合、デフォルトの STP タイプは **ibm** です。FDDI およびトークンリング VLAN の場合、デフォルトのタイプは指定されていません。
  - ソースルート トランスペアレント (SRT) 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、**ieee**
  - Source-Route Bridge (SRB) を実行している IBM STP の場合は、**ibm**
  - ソースルート トランスペアレント (SRT) 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。

表 2-37 さまざまなメディア タイプで指定できるコマンドと構文

| メディア タイプ                                 | 指定できる構文  |
|--|--|
| イーサネット                                   | <b>name vlan-name</b> 、 <b>media ethernet</b> 、 <b>state {suspend   active}</b> 、 <b>said said-value</b> 、 <b>mtu mtu-size</b> 、 <b>remote-span</b> 、 <b>tb-vlan1 tb-vlan1-id</b> 、 <b>tb-vlan2 tb-vlan2-id</b>  |
| FDDI                                     | <b>name vlan-name</b> 、 <b>media fddi</b> 、 <b>state {suspend   active}</b> 、 <b>said said-value</b> 、 <b>mtu mtu-size</b> 、 <b>ring ring-number</b> 、 <b>parent parent-vlan-id</b> 、 <b>tb-vlan1 tb-vlan1-id</b> 、 <b>tb-vlan2 tb-vlan2-id</b>  |
| FDDI-NET                                 | <b>name vlan-name</b> 、 <b>media fd-net</b> 、 <b>state {suspend   active}</b> 、 <b>said said-value</b> 、 <b>mtu mtu-size</b> 、 <b>bridge bridge-number</b> 、 <b>stp type {ieee   ibm   auto}</b> 、 <b>tb-vlan1 tb-vlan1-id</b> 、 <b>tb-vlan2 tb-vlan2-id</b><br>VTP v2 モードがディセーブルの場合、 <b>stp type</b> を <b>auto</b> に設定しないでください。   |
| トークンリング                                  | VTP v1 モードはイネーブルです。<br><b>name vlan-name</b> 、 <b>media tokenring</b> 、 <b>state {suspend   active}</b> 、 <b>said said-value</b> 、 <b>mtu mtu-size</b> 、 <b>ring ring-number</b> 、 <b>parent parent-vlan-id</b> 、 <b>tb-vlan1 tb-vlan1-id</b> 、 <b>tb-vlan2 tb-vlan2-id</b>  |
| トークンリング<br>コンセン<br>トラレー<br>機能<br>(TrCRF) | VTP v2 モードはイネーブルです。<br><b>name vlan-name</b> 、 <b>media tokenring</b> 、 <b>state {suspend   active}</b> 、 <b>said said-value</b> 、 <b>mtu mtu-size</b> 、 <b>ring ring-number</b> 、 <b>parent parent-vlan-id</b> 、 <b>bridge type {srb   srt}</b> 、 <b>are are-number</b> 、 <b>ste ste-number</b> 、 <b>backupcrf {enable   disable}</b> 、 <b>tb-vlan1 tb-vlan1-id</b> 、 <b>tb-vlan2 tb-vlan2-id</b> |
| トークンリング<br>NET                           | VTP v1 モードはイネーブルです。<br><b>name vlan-name</b> 、 <b>media tr-net</b> 、 <b>state {suspend   active}</b> 、 <b>said said-value</b> 、 <b>mtu mtu-size</b> 、 <b>bridge bridge-number</b> 、 <b>stp type {ieee   ibm}</b> 、 <b>tb-vlan1 tb-vlan1-id</b> 、 <b>tb-vlan2 tb-vlan2-id</b>   |
| トークンリング<br>ブリッジ<br>リレー<br>機能<br>(TrBRF)  | VTP v2 モードはイネーブルです。<br><b>name vlan-name</b> 、 <b>media tr-net</b> 、 <b>state {suspend   active}</b> 、 <b>said said-value</b> 、 <b>mtu mtu-size</b> 、 <b>bridge bridge-number</b> 、 <b>stp type {ieee   ibm   auto}</b> 、 <b>tb-vlan1 tb-vlan1-id</b> 、 <b>tb-vlan2 tb-vlan2-id</b>  |

表 2-38 に、VLAN の設定ルールを示します。

表 2-38 VLAN 設定ルール

| 設定   | ルール   |
|--|---|
| VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合     | すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。<br>リング番号を指定します。このフィールドを空白のままにしないでください。<br>TrCRF VLAN に同じ親 VLAN ID がある場合には一意のリング番号を指定します。1 つのバックアップ コンセントレータ リレー機能 (CRF) だけをイネーブルにすることができます。   |
| VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合 | バックアップ CRF を指定しないでください。   |
| VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合     | ブリッジ番号を指定します。このフィールドを空白のままにしないでください。  |
| VTP v1 モードはイネーブルです。                                | VLAN の STP タイプを <b>auto</b> に設定しないでください。<br>このルールは、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。  |
| トランスレーショナルブリッジングが必要な VLAN を追加する場合 (値は 0 に設定されない)   | 使用されるトランスレーショナルブリッジング VLAN ID は、すでにデータベースに存在している必要があります。<br>(たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように) コンフィギュレーションがポイントしているトランスレーショナルブリッジング VLAN ID にも、トランスレーショナルブリッジングパラメータの 1 つに元の VLAN へのポイントが含まれている必要があります。<br>コンフィギュレーションがポイントするトランスレーショナルブリッジング VLAN ID は、(たとえば、イーサネットはトークンリングをポイントすることができるというように) 元の VLAN とは異なるメディアタイプである必要があります。<br>両方のトランスレーショナルブリッジング VLAN ID が設定されている場合、(たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように) これらの VLAN は異なるメディアタイプである必要があります。 |

## 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 **ieee** です。exit config-vlan コンフィギュレーション コマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何も作用しません。

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  
Switch(config)#
```

次の例では、すべての特性をデフォルトで拡張範囲 VLAN を新規作成し、`config-vlan` モードを開始して、新しい VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する方法を示します。

```
Switch(config)# vtp mode transparent  
Switch(config)# vlan 2000  
Switch(config-vlan)# end  
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  |
|------------------------|---|
| <code>show vlan</code> | 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) のパラメータを管理ドメインに表示します。 |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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** : コマンドをデフォルト値に設定します。
- **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** : 照合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、そのデフォルトに設定します。

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。

## vlan access-map

グローバル コンフィギュレーション モードでは、**vlan filter** インターフェイス コンフィギュレーション コマンドを使用して、VLAN マップを 1 つまたは複数の VLAN に適用します。

VLAN マップ エントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

## 例

次の例では、*vac1* という名の VLAN マップを作成し、一致条件とアクションをその VLAN マップに適用する方法を示します。他のエントリがマップに存在しない場合、これはエントリ 10 になります。

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

次の例では、VLAN マップ *vac1* を削除する方法を示します。

```
Switch(config)# no vlan access-map vac1
```

## 関連コマンド

| コマンド                                | 説明  |
|-------------------------------------|---|
| <b>action</b>                       | VLAN アクセス マップ エントリのアクションを設定します。                     |
| <b>match (アクセス マップ コンフィギュレーション)</b> | 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。      |
| <b>show vlan access-map</b>         | 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。 |
| <b>vlan filter</b>                  | 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 filter

1 つ以上の VLAN に VLAN マップを適用するには、**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}
```



(注)

このコマンドは、スイッチが IP サービス イメージを稼働している場合にだけ使用できます。

## 構文の説明

|                  |   |
|------------------|---|
| <i>mapname</i>   | VLAN マップ エントリ名  |
| <i>vlan-list</i> | VLAN のリスト。  |
| <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。 |
| <b>all</b>       | 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            |
|-----------|-----------------|
| 15.0(1)EY | 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。

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  |
|--------------------------------------|---|
| <a href="#">show vlan access-map</a> | 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。           |
| <a href="#">show vlan filter</a>     | 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。 |
| <a href="#">vlan access-map</a>      | 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 メンバーシップ ポリシー サーバ (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、特権 EXEC モードで **vmps reconfirm** 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

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            |
|-----------|-----------------|
| 15.0(1)EY | 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                      |
|--|-------------------------|
| <a href="#">show vmps</a>                          | VQP および VMPS 情報を表示します。  |
| <a href="#">vmps reconfirm (グローバル コンフィギュレーション)</a> | 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 メンバーシップ ポリシー サーバ (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            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|--|---|
| <a href="#">show vmps</a>                | VQP および VMPS 情報を表示します。                            |
| <a href="#">vmps reconfirm (特権 EXEC)</a> | 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

VLAN Query Protocol (VQP) クライアントのサーバごとの再試行回数を設定するには、**vmmps 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。

**vmmps retry count**

**no vmmps retry**

|              |              |   |
|--------------|--------------|---|
| <b>構文の説明</b> | <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 メンバーシップ ポリシーサーバ (VMPS) との通信を試行する回数。指定できる範囲は 1 ~ 10 です。 |
|--------------|--------------|---|

|              |                    |
|--------------|--------------------|
| <b>デフォルト</b> | デフォルトの再試行回数は 3 です。 |
|--------------|--------------------|

|                |                   |
|----------------|-------------------|
| <b>コマンドモード</b> | グローバル コンフィギュレーション |
|----------------|-------------------|

|               |             |                 |
|---------------|-------------|-----------------|
| <b>コマンド履歴</b> | <b>リリース</b> | <b>変更箇所</b>     |
|               | 15.0(1)EY   | このコマンドが追加されました。 |

|          |   |
|----------|---|
| <b>例</b> | 次の例では、再試行回数を 7 に設定する方法を示します。<br>Switch(config)# <b>vmmps retry 7</b><br><br>設定を確認するには、 <b>show vmmps</b> 特権 EXEC コマンドを入力して、Server Retry Count 列を調べます。 |
|----------|---|

|               |                            |                        |
|---------------|----------------------------|------------------------|
| <b>関連コマンド</b> | <b>コマンド</b>                | <b>説明</b>              |
|               | <a href="#">show vmmps</a> | VQP および VMPS 情報を表示します。 |

## vmps server

プライマリ VLAN メンバーシップ ポリシー サーバ (VMPS) と最大 3 台のセカンダリ サーバを設定するには、**vmps server** グローバル コンフィギュレーション コマンドを使用します。VMPS サーバを削除するには、このコマンドの **no** 形式を使用します。

```
vmps server ipaddress [primary]
```

```
no vmps server [ipaddress]
```

### 構文の説明

|                  |  |
|------------------|--|
| <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、ドメイン ネーム システム (DNS) サーバが設定されている必要があります。 |
| <b>primary</b>   | (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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

### 使用上のガイドライン

**primary** が入力されているかどうかにかかわらず、最初に入力されたサーバは自動的にプライマリサーバとして選択されます。最初のサーバアドレスは、次のコマンドで **primary** を使用することにより無効にすることができます。

クラスタ コンフィギュレーションのメンバスイッチに IP アドレスがない場合、クラスタはそのメンバスイッチに設定された VMPS サーバを使用しません。その代わりに、クラスタはコマンドスイッチの VMPS サーバを使用し、コマンドスイッチは VMPS 要求のプロキシとなります。VMPS サーバは、クラスタを単一スイッチとして扱い、コマンドスイッチの IP アドレスを使用して要求に応答します。

*ipaddress* 値を指定せずに **no** 形式を使用すると、設定されたすべてのサーバが削除されます。ダイナミック アクセス ポートが存在するときにすべてのサーバを削除すると、スイッチは、VMPS に照会できないため、これらのポートの新しい送信元からのパケットを転送できません。

### 例

次の例では、IP アドレス 191.10.49.20 のサーバをプライマリ VMPS サーバとして設定する方法を示します。IP アドレス 191.10.49.21 および 191.10.49.22 のサーバは、セカンダリサーバとして設定されません。

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

次の例では、IP アドレス 191.10.49.21 のサーバを削除する方法を示します。

```
Switch(config)# no vmps server 191.10.49.21
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、VMPS Domain Server 列を調べます。

---

**関連コマンド**

| コマンド                      | 説明                     |
|---------------------------|------------------------|
| <a href="#">show vmps</a> | VQP および VMPS 情報を表示します。 |

## vtp (グローバル コンフィギュレーション)

VLAN トランッキング プロトコル (VTP) コンフィギュレーション特性を設定または変更するには、**vtp** グローバル コンフィギュレーション コマンドを使用します。設定を削除したり、デフォルト設定に戻したりする場合は、このコマンドの **no** 形式を使用します。

```
vtp {domain domain-name | file filename | interface name [only] | mode {client | off | server |
transparent} [mst | unknown | vlan] | password password [hidden | secret] | pruning |
version number}
```

```
no vtp {file | interface | mode [client | off | server | transparent] [mst | unknown | vlan] | password
| pruning | version}
```

### 構文の説明

|                                  |   |
|----------------------------------|---|
| <b>domain</b> <i>domain-name</i> | スイッチの VTP 管理ドメインを識別する 1 ~ 32 文字の ASCII 文字列で VTP ドメイン名を指定します。ドメイン名では大文字と小文字が区別されます。  |
| <b>file</b> <i>filename</i>      | VTP VLAN 設定が保存されている Cisco IOS ファイル システム ファイルを指定します。   |
| <b>interface</b> <i>name</i>     | このデバイスで更新された VTP ID を提供するインターフェイスの名前を指定します。   |
| <b>only</b>                      | (任意) VTP IP アップデータとしてこのインターフェイスの IP アドレスだけで使用します。   |
| <b>mode</b>                      | VTP 装置モードをクライアント、サーバ、またはトランスペアレントに指定します。  |
| <b>client</b>                    | スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信できますが、VLAN 設定を格納するために必要な不揮発性メモリがありません。スイッチで VLAN を設定することはできません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。   |
| <b>off</b>                       | スイッチを VTP オフ モードにします。VTP オフ モードのスイッチは、トランク ポート上で VTP アドバタイズメントを転送しないことを除いて、VTP トランスペアレント デバイスと同様に機能します。   |
| <b>server</b>                    | スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信します。スイッチでは VLAN を設定できます。スイッチは、再起動後に、不揮発性メモリから現在の VTP データベース内のすべての VLAN 情報を回復できます。   |
| <b>transparent</b>               | スイッチを VTP トランスペアレント モードにします。VTP トランスペアレント モードのスイッチは、VTP に対してディセーブルであり、アドバタイズの送信や、他のデバイスから送信されたアドバタイズからの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定に影響を与えることはありません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。<br><br>VTP モードがトランスペアレントである場合、モードおよびドメイン名はスイッチの実行コンフィギュレーション ファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、 <b>copy running-config startup-config</b> 特権 EXEC コマンドを入力します。 |

|                                 |   |
|---------------------------------|---|
| <b>mst</b>                      | (任意) マルチ スパニング ツリー (MST) VTP データベース (VTP バージョン 3 に限る) にモードを設定します。   |
| <b>unknown</b>                  | (任意) 未知の VTP データベース (VTP バージョン 3 に限る) にモードを設定します。   |
| <b>vlan</b>                     | (任意) VLAN VTP データベースにモードを設定します。これがデフォルトです (VTP バージョン 3 に限る)。  |
| <b>password <i>password</i></b> | VTP アドバタイズで送信され、受信 VTP アドバタイズを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ~ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。  |
| <b>hidden</b>                   | (任意) パスワード ストリングから生成されたキーが VLAN データベース ファイルに保存されることを指定します。 <b>hidden</b> キーワードを指定しない場合、パスワード ストリングはクリア テキストに保存されます。 <b>hidden</b> パスワードを入力した場合、そのパスワードを再入力し、ドメイン内でコマンドを発行する必要があります。このキーワードは VTP バージョン 3 のみサポートされます。 |
| <b>secret</b>                   | (任意) ユーザがパスワードの秘密キーを直接設定できるようにします (VTP バージョン 3 に限る)。  |
| <b>pruning</b>                  | スイッチ上で VTP プルーニングをイネーブルにします。  |
| <b>version <i>number</i></b>    | VTP バージョンをバージョン 1、バージョン 2、またはバージョン 3 に設定します。  |

**デフォルト**

デフォルトのファイル名は *flash:vlan.dat* です。

デフォルト モードはサーバ モードで、デフォルトのデータベースは VLAN です。

VTP バージョン 3 では、MST データベースのデフォルト モードはトランスペアレントです。

ドメイン名またはパスワードは定義されていません。

パスワードは設定されていません。

プルーニングはディセーブルです。

デフォルトのバージョンはバージョン 1 です。

**コマンド モード**

グローバル コンフィギュレーション

**コマンド履歴**

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

VTP モード、ドメイン名、および VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードがトランスペアレントであり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ VTP モードがサーバ モードの場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 の VLAN の VTP モードおよび VLAN 設定は、VLAN データベース情報によって選択され、1005 を超える VLAN は、スイッチ コンフィギュレーション ファイルから設定されます。

新規データベースをロードするのに **vtp file filename** を使用することはできません。これは、既存のデータベースが保存されているファイルの名前を変更するだけです。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、スイッチは非管理ドメイン ステートの状態です。非管理ドメイン ステートの間は、ローカル VLAN 設定に変更が生じて、スイッチは VTP アドバタイズを送信しません。スイッチは、トランッキングを行っているポートで最初の VTP サマリー パケットを受信した後、または **vtp domain** コマンドでドメイン名を設定した後で、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信した場合、そのコンフィギュレーション リビジョン番号を 0 にリセットします。スイッチが非管理ドメイン ステートから抜け出したあと、NVRAM (不揮発性 RAM) をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てのしかありません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、スイッチを VTP サーバ モードに戻すことができます。
- **vtp mode server** コマンドは、スイッチがクライアント モードまたはトランスペアレント モードでない場合にエラーを返さないことを除けば、**no vtp mode** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバのコンフィギュレーションをコピーします。クライアント モードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。受信スイッチがサーバ モードまたはトランスペアレント モードである場合、スイッチの設定は変更されません。
- トランスペアレント モードのスイッチは、VTP に参加しません。トランスペアレント モードのスイッチで VTP または VLAN 設定の変更を行った場合、変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードのスイッチで VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべてのスイッチに伝播されます。
- **vtp mode transparent** コマンドは、ドメインの VTP をディセーブルにしますが、スイッチからドメインを削除しません。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN を追加したり、VTP および VLAN 情報を実行コンフィギュレーション ファイルに保存したりする場合には、VTP モードはトランスペアレントに設定してください。VTP は拡張範囲 VLAN をクライアントおよびサーバ モードでサポートし、VLAN データベースに保存します。

- VTP バージョン 1 および 2 では、拡張範囲 VLAN がスイッチで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラー メッセージが表示され、その設定は許可されません。VTP モードは、VTP バージョン 3 で拡張 VLAN を使用することにより変更できます。
- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバ モードまたはクライアント モードのいずれかに限ります。
- **vtp mode off** コマンドを使用すると、デバイスをオフに設定します。**no vtp mode off** コマンドを使用すると、デバイスを VTP サーバ モードにリセットします。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードでは、大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのスイッチで一致している必要があります。
- スイッチをパスワードが設定されていない状態に戻す場合は、このコマンドの **no vtp password** 形式を使用します。
- **hidden** および **secret** キーワードは、VTP バージョン 3 だけでサポートされています。VTP バージョン 2 から VTP バージョン 3 に変換する場合、変換前に **hidden** または **secret** キーワードを削除する必要があります。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
- VTP サーバでプルーニングをイネーブルにすると、プルーニングは VLAN ID 1 ~ 1005 の管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョンを設定するときには、次の注意事項に従ってください。

- バージョン 2 (v2) モード ステートを切り替えると、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP スイッチは他のすべての VTP デバイスの機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP スイッチでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼働するように設定する必要があります。
- ドメイン内のすべてのスイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応スイッチに伝播されます。
- トークンリング環境で VTP を使用している場合、VTP バージョン 2 もイネーブルである必要があります。
- Token Ring Bridge Relay Function (TrBRF) または Token Ring Concentrator Relay Function (TrCRF) VLAN メディア タイプを設定している場合には、バージョン 2 を使用してください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。
- VTP バージョン 3 では、VLAN データベース情報だけでなく、すべてのデータベース VTP 情報が VTP ドメインに伝播します。
- トランスペアレント モードでは、2 個の VTP バージョン 3 リージョンしか VTP バージョン 1 または VTP バージョン 2 を超えて通信できません。

スイッチ コンフィギュレーション ファイルにパスワード、プルーニング、およびバージョン コンフィギュレーションを保存することはできません。

## vtp (グローバル コンフィギュレーション)

## 例

次の例では、VTP コンフィギュレーション メモリのファイル名を *vtpfilename* に変更する方法を示します。

```
Switch(config)# vtp file vtpfilename
```

次の例では、デバイス ストレージのファイル名をクリアする方法を示します。

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

次の例では、このデバイスの VTP アップデータ ID を提供するインターフェイスの名前を指定する方法を示します。

```
Switch(config)# vtp interface gigabitethernet
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(config)# vtp domain OurDomainName
```

次の例では、スイッチを VTP トランスペアレント モードにする方法を示します。

```
Switch(config)# vtp mode transparent
```

次の例では、VTP ドメイン パスワードを設定する方法を示します。

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

次の例では、VLAN データベースでのプルーンングをイネーブルにする方法を示します。

```
Switch(config)# vtp pruning
Pruning switched ON
```

次の例では、VLAN データベースのバージョン 2 モードをイネーブルにする方法を示します。

```
Switch(config)# vtp version 2
```

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

## 関連コマンド

| コマンド                                  | 説明   |
|---------------------------------------|--|
| <b>show vtp status</b>                | スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。 |
| <b>vtp (インターフェイス<br/>コンフィギュレーション)</b> | インターフェイスで VTP をイネーブルまたはディセーブルにします。             |

# vtp (インターフェイス コンフィギュレーション)

ポート単位で VLAN トランッキング プロトコル (VTP) をイネーブルにするには、**vtp** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで VTP をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**vtp**

**no vtp**



(注)

このコマンドは、スイッチが LAN ベース イメージおよび VTP バージョン 3 を実行している場合だけサポートされます。

## 構文の説明

このコマンドには、キーワードと引数はありません。

## デフォルト

なし

## コマンドモード

インターフェイス コンフィギュレーション

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、VTP バージョン 3 に設定されているスイッチ上だけでサポートされています。

## 例

次の例では、インターフェイス上で VTP をイネーブルにする方法を示します。

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

次の例では、インターフェイス上で VTP をディセーブルにする方法を示します。

```
Switch(config-if)# no vtp
```

## 関連コマンド

| コマンド                                    | 説明  |
|---|---|
| <a href="#">vtp (グローバル コンフィギュレーション)</a> | VTP のドメイン名、パスワード、プルーニング、バージョン、およびモードをグローバルに設定します。 |

# vtp primary

VLAN トランッキング プロトコル (VTP) のプライマリ サーバとしてスイッチを設定するには、**vtp primary** 特権 EXEC コマンドを使用します。

**vtp primary [mst | vlan] [force]**

このコマンドには、**no** 形式はありません。



(注)

このコマンドは、スイッチが LAN ベース イメージおよび VTP バージョン 3 を実行している場合だけサポートされます。



(注)

**vtp {password *password* | pruning | version *number*}** コマンドはコマンドライン ヘルプに表示されませんが、サポートされていません。

## 構文の説明

|              |  |
|--------------|--|
| <b>mst</b>   | (任意) スイッチをマルチ スパニングツリー (MST) 機能のプライマリ VTP サーバとして設定します。 |
| <b>vlan</b>  | (任意) スイッチを VLAN のプライマリ VTP サーバとして設定します。                |
| <b>force</b> | (任意) プライマリ サーバを設定する場合、スイッチが競合するデバイスをチェックしないように設定します。   |

## デフォルト

スイッチは VTP セカンダリ サーバです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、VTP バージョン 3 に設定されているスイッチ上だけでサポートされています。

VTP プライマリ サーバはデータベース情報をアップデートし、システム内のすべてのデバイスによって行われるアップデートを送信します。VTP セカンダリ サーバは、プライマリ サーバから受信したアップデートされた VTP のコンフィギュレーションを NVRAM にバックアップすることだけができます。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。プライマリ サーバのステータスは、管理者がドメイン内のテイクオーバー メッセージを発行する場合のデータベース アップデートのためだけに必要です。プライマリ サーバなしで実用 VTP ドメインを持つことができます。

デバイスがリロードするかドメイン パラメータが変更された場合、プライマリ サーバのステータスは失われます。

**例** 次の例では、スイッチを VLAN のプライマリ VTP サーバとして設定する方法を示します。

```
Switch# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

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

#### 関連コマンド

| コマンド                           | 説明   |
|--------------------------------|--|
| <b>show vtp status</b>         | スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。 |
| <b>vtp (グローバル コンフィギュレーション)</b> | VTP ファイル名、インターフェイス、ドメイン名、モード、およびバージョンを設定します。   |

■ vtp primary



# APPENDIX A

## IE 2000 スイッチのブートローダ コマンド

この付録では、スイッチのブートローダ コマンドについて説明します。

通常のブートローダ処理中は、ブートローダ 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 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。

ブートローダにアクセスするには、次の手順を実行します。

- ステップ 1** スイッチの起動中、**Express Setup** ボタンを押したままにします。
- ステップ 2** LED (システム、アラーム、セットアップ) が赤色に変化したら、**Express Setup** ボタンから手を放します。LED が消灯します。
- ステップ 3** 再度、**Express Setup** ボタンを押したままにします。
- ステップ 4** LED (システム、アラーム、セットアップ) が再度赤色に変化したら、**Express Setup** ボタンから手を放します。

# boot

実行可能イメージをロードおよび起動して、コマンドライン インターフェイスを開始するには、**boot** ブートローダ コマンドを使用します。

```
boot [-post | -n | -p | flag] filesystem:/file-url ...
```

## 構文の説明

|                             |  |
|-----------------------------|--|
| <b>-post</b>                | (任意) 拡張および総合 POST (電源投入時自己診断テスト) 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。 |
| <b>-n</b>                   | (任意) 起動後すぐに、Cisco IOS デバッガが休止します。  |
| <b>-p</b>                   | (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。   |
| <b><i>flag</i></b>          | (任意) システムの再起動時に使用されるブート フラグを設定します。   |
| <b><i>filesystem:</i></b>   | 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 <b>flash:</b> を使用します。                        |
| <b><i>/file-url ...</i></b> | (任意) ブート可能イメージのパス (ディレクトリ) および名前です。各イメージ名はセミコロンで区切ります。                                     |

## デフォルト

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

## コマンド モード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

引数を何も指定しないで **boot** コマンドを入力した場合、スイッチは、BOOT 環境変数が設定されていればその中の情報を使用して、システムを自動的に起動しようとします。**file-url** 変数にイメージ名を指定した場合、**boot** コマンドは指定されたイメージを起動しようとします。

ブートローダ **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 セッションだけに適用されます。これらの設定が保存されて、次の起動処理に使用されることはありません。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

## 例

次の例では、*new-image.bin* イメージを使用してスイッチを起動する方法を示します。

```
switch: boot flash:/new-images/new-image.bin
```

このコマンドを入力すると、セットアップ プログラムを開始するように求められます。

| 関連コマンド | コマンド                | 説明   |
|--------|---------------------|--|
|        | <a href="#">set</a> | コマンドに <b>BOOT</b> 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 <b>BOOT</b> 環境変数を設定します。 |

# cat

1 つまたは複数のファイルの内容を表示するには、**cat** ブートローダ 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 <b>flash:</b> 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。                      |

## デフォルト

なし

## コマンドモード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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、バックアップ コンフィギュレーション ファイルの内容を表示する方法と出力例を示します。

```
switch: cat flash:config_backup

!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Switch

switch: cat flash:/ies-lanbase-mz.122-44.EX/info
version_suffix: lanbase-122-44.EX
version_directory: ies-lanbase-mz.122-44.EX
image_system_type_id: 0x00000000
image_name: ies-lanbase-mz.122-44.EX.bin
ios_image_file_size: 6369792
total_image_file_size: 11878912
image_feature: LAYER_2|MIN_DRAM_MEG=64
image_family: IES
stacking_number: 1.37
board_ids: 0x00000090 0x00000091
info_end:
```

| 関連コマンド | コマンド                 | 説明                      |
|--------|----------------------|-------------------------|
|        | <a href="#">more</a> | 1 つまたは複数のファイルの内容を表示します。 |
|        | <a href="#">type</a> | 1 つまたは複数のファイルの内容を表示します。 |

# copy

コピー元からコピー先へとファイルをコピーするには、**copy** ブートローダ 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>-b block-size</b>         | (任意) このオプションは、内部開発およびテスト専用です。                                       |
| <b>filesystem:</b>           | 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 <b>flash:</b> を使用します。 |
| <b>/source-file-url</b>      | コピー元のパス (ディレクトリ) およびファイル名です。  |
| <b>/destination-file-url</b> | 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

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 コマンドを入力します。

## 関連コマンド

| コマンド          | 説明                                    |
|---------------|---------------------------------------|
| <b>delete</b> | 指定されたファイル システムから 1 つまたは複数のファイルを削除します。 |

# delete

指定したファイル システムから 1 つまたは複数のファイルを削除するには、**delete** ブートローダ 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 <b>flash:</b> 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。                      |

デフォルト なし

コマンド モード ブートローダ

| コマンド履歴 | リリース      | 変更箇所            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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 コマンドを入力します。

| 関連コマンド | コマンド                 | 説明                      |
|--------|----------------------|-------------------------|
|        | <a href="#">copy</a> | コピー元からコピー先にファイルをコピーします。 |

# dir

指定したファイル システム内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 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 <b>flash:</b> 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。           |

## デフォルト

なし

## コマンドモード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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"><li>• d : ディレクトリ</li><li>• r : 読み取り可能</li><li>• w : 書き込み可能</li><li>• x : 実行可能</li></ul> |
| 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                     |
|-----------------------|------------------------|
| <a href="#">mkdir</a> | 1 つまたは複数のディレクトリを作成します。 |
| <a href="#">rmdir</a> | 1 つまたは複数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 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

### コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

### 使用上のガイドライン

フラッシュ ファイル システムは、通常の起動プロセス中に自動的に初期化されます。

このコマンドは、フラッシュ ファイル システムを手動で初期化します。たとえば、パスワードを忘れた場合には、回復手順中にこのコマンドを使用します。

# format

指定したファイル 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削除するには、**format** ブートローダ コマンドを使用します。

**format** *filesystem:*

|       |                    |   |
|-------|--------------------|---|
| 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 <b>flash:</b> を使用します。 |
|-------|--------------------|---|

|       |    |
|-------|----|
| デフォルト | なし |
|-------|----|

|          |        |
|----------|--------|
| コマンド モード | ブートローダ |
|----------|--------|

| コマンド履歴 | リリース      | 変更箇所            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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整合性を確認するには、**fsck** ブートローダ コマンドを使用します。

**fsck [-test | -f] filesystem:**

## 構文の説明

|                    |   |
|--------------------|---|
| <b>-test</b>       | (任意) ファイル システム コードを初期化し、フラッシュ メモリ上で新たに 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)。 |
| <b>-f</b>          | (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 セクタ内の巡回冗長検査 (CRC) は実行されません。                           |
| <b>filesystem:</b> | 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 <b>flash:</b> を使用します。                                     |

## デフォルト

なし

## コマンド デフォルト

ファイル システム チェックは実行されません。

## コマンド モード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 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。

### デフォルト

なし

### コマンド モード

ブートローダ

### コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 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 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。

### デフォルト

なし

### コマンドモード

ブートローダ

### コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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

指定したファイル システムに 1 つまたは複数のディレクトリを新規作成するには、**mkdir** ブートローダ 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 <b>flash:</b> 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せん。                                |

## デフォルト

なし

## コマンド モード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 コマンドを入力します。

## 関連コマンド

| コマンド         | 説明                                      |
|--------------|---|
| <b>dir</b>   | 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。 |
| <b>rmdir</b> | 指定されたファイル システムから 1 つまたは複数のディレクトリを削除します。 |

# more

1 つまたは複数のファイルの内容を表示するには、**more** ブートローダ コマンドを使用します。

**more filesystem:/file-url ...**

## 構文の説明

|                      |  |
|----------------------|--|
| <b>filesystem:</b>   | 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 <b>flash:</b> を使用します。 |
| <b>/file-url ...</b> | 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。                     |

## デフォルト

なし

## コマンドモード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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、コンフィギュレーション バックアップ ファイルの内容を表示する方法を示します。

```
switch: more flash:/ies-lanbase-mz.122-44.EX/info
version_suffix: lanbase-122-44.EX
version_directory: ies-lanbase-mz.122-44.EX
image_system_type_id: 0x00000000
image_name: ies-lanbase-mz.122-44.EX.bin
ios_image_file_size: 6369792
total_image_file_size: 11878912
image_feature: LAYER_2|MIN_DRAM_MEG=64
image_family: IES
stacking_number: 1.37
board_ids: 0x00000090 0x00000091
info_end:
```

## 関連コマンド

| コマンド        | 説明                      |
|-------------|-------------------------|
| <b>cat</b>  | 1 つまたは複数のファイルの内容を表示します。 |
| <b>type</b> | 1 つまたは複数のファイルの内容を表示します。 |

# rename

ファイル名を変更するには、**rename** ブートローダ 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 <b>flash:</b> 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。  |

## デフォルト

なし

## コマンド モード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 コマンドを入力します。

## 関連コマンド

| コマンド                 | 説明                      |
|----------------------|-------------------------|
| <a href="#">copy</a> | コピー元からコピー先にファイルをコピーします。 |

# reset

システムでハードリセットを実行するには、**reset** ブートローダ 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。

## デフォルト

なし

## コマンドモード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|----------------------|---|
| <a href="#">boot</a> | 実行可能イメージをロードおよび起動して、コマンドライン インターフェイスを開始します。 |

# rmdir

指定したファイル システムから 1 つまたは複数の空のディレクトリを削除するには、**rmdir** ブートローダ 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 <b>flash:</b> 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。                 |

## デフォルト

なし

## コマンド モード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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 コマンドを入力します。

## 関連コマンド

| コマンド         | 説明                                       |
|--------------|--|
| <b>dir</b>   | 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。  |
| <b>mkdir</b> | 指定されたファイル システムに 1 つまたは複数のディレクトリを新規作成します。 |

# set

ブートローダまたはスイッチ上で稼働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 コマンドを使用します。

**set variable value**

## 構文の説明

*variable value* *variable* および *value* には、次に示すキーワードのいずれかを使用します。

**MANUAL\_BOOT** : スイッチを自動で起動するか、または手動で起動するかを決定します。

有効値は 1、yes、0、および no です。no または 0 に設定されている場合、ブートローダはシステムを自動的に起動しようとします。それ以外に設定されている場合は、ブートローダ モードから手動でスイッチを起動する必要があります。

**BOOT filesystem:/file-url** : 自動起動時にロードおよび実行される実行可能ファイルのセミコロン区切りリストです。

BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 環境変数が設定されていても指定されたイメージをロードできない場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとします。

**ENABLE\_BREAK** : コンソール上の Break キーを使用して自動起動プロセスを中断できるかどうかを決定します。

有効値は 1、yes、on、0、no、および off です。1、yes、または on に設定されている場合は、フラッシュ ファイル システムの初期化後にコンソール上で Break キーを押して、自動起動プロセスを中断できます。

**HELPER filesystem:/file-url** : ブートローダ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 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からボー レート設定を継承し、この値を引き続き使用します。指定できる範囲は 0 ~ 4294967295 bps です。有効値は、50、75、110、150、300、600、1200、1800、2000、2400、3600、4800、7200、9600、14400、19200、28800、38400、56000、57600、115200、および 128000 です。

最も一般的な値は、300、1200、2400、9600、19200、57600、および 115200 です。

**HELPER\_CONFIG\_FILE filesystem:/file-url** : Cisco IOS ヘルパー イメージで使用されるコンフィギュレーション ファイルの名前です。この名前が設定されていない場合は、CONFIG\_FILE 環境変数で指定されたファイルが、ロードされるすべてのバージョンの Cisco IOS (ヘルパー イメージを含む) で使用されます。この変数は、内部開発およびテスト専用です。

**デフォルト**

環境変数のデフォルト値は、次のとおりです。

MANUAL\_BOOT: No (0)

BOOT: ヌル ストリング

ENABLE\_BREAK: no (off または 0) (コンソール上で Break キーを押して自動起動プロセスを中断することはできません)

HELPER: デフォルト値はありません (ヘルパー ファイルは自動的にロードされません)。

PS1: switch:

CONFIG\_FILE: config.text

BAUD: 9600 bps

HELPER\_CONFIG\_FILE: デフォルト値はありません (ヘルパー コンフィギュレーション ファイルは指定されません)

SWITCH\_NUMBER: 1

SWITCH\_PRIORITY: 1



(注)

値が設定された環境変数は、各ファイルのフラッシュ ファイル システムに保存されています。これらのファイルの各行に、環境変数名と等号、その後に変数の値が格納されています。このファイルに表示されていない変数には値がありません。表示されていればヌル ストリングであっても値があります。ヌル ストリング (たとえば "") に設定されている変数は、値が設定された変数です。多くの環境変数は事前に定義されており、デフォルト値が設定されています。

**コマンド モード**

ブートローダ

**コマンド履歴**

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | 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。

通常的环境中では、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 コマンドを使用します。

#### 関連コマンド

| コマンド                  | 説明                       |
|-----------------------|--------------------------|
| <a href="#">unset</a> | 1 つまたは複数の環境変数を元の設定に戻します。 |

# type

1 つまたは複数のファイルの内容を表示するには、**type** ブートローダ 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 <b>flash:</b> 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。                      |

デフォルト なし

コマンド モード ブートローダ

| コマンド履歴 | リリース      | 変更箇所            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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:config_backup

!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Switch

switch: type flash:/ies-lanbase-mz.122-44.EX/info
version_suffix: lanbase-122-44.EX
version_directory: ies-lanbase-mz.122-44.EX
image_system_type_id: 0x00000000
image_name: ies-lanbase-mz.122-44.EX.bin
ios_image_file_size: 6369792
total_image_file_size: 11878912
image_feature: LAYER_2|MIN_DRAM_MEG=64
image_family: IES
stacking_number: 1.37
board_ids: 0x00000090 0x00000091
info_end:
```

## ■ type

| 関連コマンド | コマンド                 | 説明                      |
|--------|----------------------|-------------------------|
|        | <a href="#">cat</a>  | 1 つまたは複数のファイルの内容を表示します。 |
|        | <a href="#">more</a> | 1 つまたは複数のファイルの内容を表示します。 |

# unset

1 つまたは複数の環境変数をリセットするには、**unset** ブートローダ コマンドを使用します。

**unset variable ...**

## 構文の説明

*variable*

*variable* には、次に示すキーワードのいずれかを使用します。

**MANUAL\_BOOT** : スイッチを自動で起動するか、または手動で起動するかを決定します。

**BOOT** : 自動起動時に、実行可能ファイルのリストをリセットして、ロードおよび実行します。**BOOT** 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。**BOOT** 環境変数が設定されていても指定されたイメージをロードできない場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとします。

**ENABLE\_BREAK** : フラッシュ ファイル システムの初期化後に、コンソール上の **Break** キーを使用して自動起動プロセスを中断できるかどうかを決定します。

**HELPER** : ブートローダ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、ブートローダの機能を拡張したり、パッチを当てたりします。

**PS1** : ブートローダ モードの場合に、コマンドライン プロンプトとして使用される文字列です。

**CONFIG\_FILE** : Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名をリセットします。

**BAUD** : コンソールで使用される速度 (ビット/秒単位) をリセットします。コンフィギュレーション ファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボー レート設定を継承し、この値を引き続き使用します。

**HELPER\_CONFIG\_FILE** : Cisco IOS ヘルパー イメージで使用されるコンフィギュレーション ファイルの名前をリセットします。この名前が設定されていない場合は、**CONFIG\_FILE** 環境変数で指定されたファイルが、ロードされるすべてのバージョンの Cisco IOS (ヘルパー イメージを含む) で使用されます。この変数は、内部開発およびテスト専用です。

## デフォルト

なし

## コマンド モード

ブートローダ

## コマンド履歴

リリース

変更箇所

15.0(1)EY

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、**no boot manual** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

BOOT 環境変数は、**no boot system** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

ENABLE\_BREAK 環境変数は、**no boot enable-break** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

HELPER 環境変数は、**no boot helper** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

CONFIG\_FILE 環境変数は、**no boot config-file** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

HELPER\_CONFIG\_FILE 環境変数は、**no boot helper-config-file** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

ブートローダのプロンプト文字列 (PS1) には、等号 (=) を除く、出力可能な文字列を 120 文字まで指定できます。

**例**

次の例では、プロンプト文字列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               |
|---------------------|------------------|
| <a href="#">set</a> | 環境変数を設定または表示します。 |

# version

ブートローダのバージョンを表示するには、**version** ブートローダ 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。

## デフォルト

なし

## コマンド モード

ブートローダ

## コマンド履歴

| リリース      | 変更箇所            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 例

次の例では、ブートローダのバージョンを表示する方法を示します。

```
switch: version  
IE2000 Boot Loader (IE2000-HBOOT-M) Version 15.0(1)EY  
Compiled Wed 05-Mar-08 10:11 by engineer
```

■ version



## APPENDIX **B**

# IE 2000 スイッチ デバッグ コマンド

---

この付録では、スイッチ用に作成または変更された **debug** 特権 EXEC コマンドについて説明します。これらのコマンドは、インターネットワーキングの問題の診断および解決に役立ちます。使用する場合には、必ずシスコのテクニカル サポート担当者の指示に従ってください。



### 注意

---

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。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。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

---

# debug authentication

インターフェイスの認証設定のデバッグをイネーブルにするには、特権 EXEC モードで **debug authentication** を使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug authentication {all | errors | events | sync | feature [all] [acct] [auth_fail_vlan]
                    [auth_policy] [autocfg] [critical] [dhcp] [guest_vlan] [mab_pm] [mda] [multi_auth]
                    [switch_pm] [switch_sync] [vlan_assign] [voice] [webauth] [all | errors | events]}
```

```
no debug authentication {all | errors | events | sync | feature [all] [acct] [auth_fail_vlan]
                       [auth_policy] [autocfg] [critical] [dhcp] [guest_vlan] [mab_pm] [mda] [multi_auth]
                       [switch_pm] [switch_sync] [vlan_assign] [voice] [webauth] [all | errors | events]}
```

## 構文の説明

|                       |  |
|-----------------------|--|
| <b>all</b>            | (任意) 認証マネージャ デバッグ メッセージをすべて表示します。  |
| <b>errors</b>         | (任意) 認証マネージャ エラー デバッグ メッセージをすべて表示します。  |
| <b>events</b>         | (任意) すべての認証マネージャ イベントのデバッグ メッセージ (レジストリおよび各種イベントを含む) を表示します。   |
| <b>sync</b>           | (任意) 操作同期認証マネージャ デバッグ メッセージを表示します。   |
| <b>feature</b>        | (任意) 認証マネージャ機能のデバッグ メッセージを表示します。   |
| <b>acct</b>           | (任意) 表示認証マネージャ アカウンティング情報を表示します。   |
| <b>auth_fail_vlan</b> | (任意) 制限された VLAN の認証マネージャ エラーを表示します。  |
| <b>auth_policy</b>    | (任意) 認証ポリシー メッセージを表示します。   |
| <b>autocfg</b>        | (任意) 自動設定認証マネージャ デバッグ メッセージを表示します。   |
| <b>critical</b>       | (任意) アクセス不能な認証バイパス メッセージを表示します。<br><br>(注) アクセス不能な認証バイパス機能は、クリティカル認証または認証、許可、アカウンティング (AAA) 失敗ポリシーとも呼ばれています。 |
| <b>dhcp</b>           | (任意) DHCP ダイナミック アドレス対応インターフェイスでの認証マネージャ デバッグ メッセージを表示します。   |
| <b>guest_vlan</b>     | (任意) ゲスト VLAN 認証マネージャ メッセージを表示します。   |
| <b>mab_pm</b>         | (任意) MAC 認証マネージャ バイパス認証デバッグ メッセージを表示します。   |
| <b>mda</b>            | (任意) 表示マルチドメイン認証マネージャ デバッグ メッセージを表示します。  |
| <b>multi_auth</b>     | (任意) マルチ認証マネージャ デバッグ認証メッセージを表示します。   |
| <b>switch_pm</b>      | (任意) スイッチ ポート マネージャ メッセージを表示します。   |
| <b>switch_sync</b>    | (任意) スイッチ、認証サーバ、および接続装置の間の同期メッセージを表示します。   |
| <b>vlan_assign</b>    | (任意) VLAN 割り当てデバッグ メッセージを表示します。  |
| <b>voice</b>          | (任意) 音声 VLAN デバッグ メッセージを表示します。   |
| <b>webauth</b>        | (任意) Web 認証マネージャ デバッグ メッセージを表示します。   |

## デフォルト

認証デバッグはディセーブルです。

## コマンドモード

特権 EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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 authentication` コマンドは、`no debug authentication` コマンドと同じです。

| 関連コマンド | コマンド  | 説明  |
|--------|---|---|
|        | <code>authentication control-direction</code> | ポート モードを単一方向または双方向に設定します。   |
|        | <code>authentication event</code>             | 特定の認証イベントのアクションを設定します。  |
|        | <code>authentication fallback</code>          | 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。        |
|        | <code>authentication host-mode</code>         | ポートで認証マネージャ モードを設定します。  |
|        | <code>authentication open</code>              | 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。   |
|        | <code>authentication order</code>             | ポートで使用する認証方式の順序を設定します。  |
|        | <code>authentication periodic</code>          | 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。   |
|        | <code>authentication port-control</code>      | 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。   |
|        | <code>authentication priority</code>          | ポート プライオリティ リストに認証方式を追加します。   |
|        | <code>authentication violation</code>         | 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。 |
|        | <code>show authentication</code>              | スイッチの認証マネージャ イベントに関する情報を表示します。  |

# debug auto qos

Automatic Quality of Service (auto-QoS) 機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug auto qos** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug auto qos**

**no debug auto qos**



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

このコマンドには、キーワードと引数はありません。

## デフォルト

auto-QoS デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。特権 EXEC モードで **debug auto qos** コマンドを入力して、デバッグをイネーブルにします。

**undebug auto qos** コマンドは、**no debug auto qos** コマンドと同じです。

## 例

次の例では、auto-QoS がイネーブルの場合に自動的に生成される QoS 設定を表示する方法を示します。

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-phone

21:29:41: mls qos map cos-dscp 0 8 16 26 32 46 48 56
21:29:41: mls qos
21:29:42: no mls qos srr-queue input cos-map
21:29:42: no mls qos srr-queue output cos-map
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 3 0
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 2 1
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 1 2
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
21:29:43: mls qos srr-queue input cos-map queue 2 threshold 3 3 5
21:29:43: mls qos srr-queue output cos-map queue 1 threshold 3 5
21:29:43: mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
```

```

21:29:44: mls qos srr-queue output cos-map queue 3 threshold 3 2 4
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 2 1
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 3 0
21:29:44: no mls qos srr-queue input dscp-map
21:29:44: no mls qos srr-queue output dscp-map
21:29:44: mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 32
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
21:29:48: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 1 8
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
21:29:49: no mls qos srr-queue input priority-queue 1
21:29:49: no mls qos srr-queue input priority-queue 2
21:29:50: mls qos srr-queue input bandwidth 90 10
21:29:50: no mls qos srr-queue input buffers
21:29:50: mls qos queue-set output 1 buffers 10 10 26 54
21:29:50: interface GigabitEthernet1/1
21:29:50: mls qos trust device cisco-phone
21:29:50: mls qos trust cos
21:29:50: no queue-set 1
21:29:50: srr-queue bandwidth shape 10 0 0 0
21:29:50: srr-queue bandwidth share 10 10 60 20

```

## 関連コマンド

| コマンド                  | 説明   |
|-----------------------|--|
| <b>auto qos voip</b>  | QoS ドメイン内で Voice over IP (VoIP) の auto-QoS を設定します。   |
| <b>show auto qos</b>  | auto-QoS 機能によって生成された初期設定を表示します。  |
| <b>show debugging</b> | 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。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# 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、特権 EXEC モードで **debug backup** 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

|                            |   |
|----------------------------|---|
| <b>all</b>                 | すべてのバックアップ インターフェイスのデバッグ メッセージを表示します。     |
| <b>errors</b>              | 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。 |
| <b>events</b>              | 表示バックアップ インターフェイス イベント デバッグ メッセージを表示します。  |
| <b>vlan-load-balancing</b> | バックアップ インターフェイスの VLAN ロード バランシングを表示します。   |

## デフォルト

バックアップ インターフェイス デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug cip

Common Industrial Protocol (CIP) サブシステムのデバッグをイネーブルにするには、特権 EXEC モードで **debug cip** 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 cip {assembly | connection manager | errors | event | file | io | packet | request response |
security | session | socket}
```

```
no debug cip {assembly | connection manager | errors | event | file | io | packet | request response
| security | session | socket}
```

## 構文の説明

|                           |                                  |
|---------------------------|----------------------------------|
| <b>assembly</b>           | CIP アセンブリのデバッグ メッセージを表示します。      |
| <b>connection manager</b> | CIP 接続マネージャのデバッグ メッセージを表示します。    |
| <b>errors</b>             | CIP エラー デバッグ メッセージを表示します。        |
| <b>event</b>              | CIP イベント デバッグ メッセージを表示します。       |
| <b>file</b>               | CIP ファイルのデバッグ メッセージを表示します。       |
| <b>io</b>                 | CIP 入出力 (I/O) のデバッグ メッセージを表示します。 |
| <b>packet</b>             | CIP パケットのデバッグ メッセージを表示します。       |
| <b>request response</b>   | CIP 要求応答のデバッグ メッセージを表示します。       |
| <b>security</b>           | CIP セキュリティのデバッグ メッセージを表示します。     |
| <b>session</b>            | CIP セッションのデバッグ メッセージを表示します。      |
| <b>socket</b>             | CIP ソケットのデバッグ メッセージを表示します。       |

## デフォルト

CIP デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**undebug cip** コマンドは、**no debug cip** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show cip</b>       | Common Industrial Protocol (CIP) サブシステムに関する情報を表示します。  |
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug cisp

クライアント情報のデバッグ メッセージ交換およびイベントをイネーブルにするには、**debug cisp** グローバル Configuration Command Signalling Protocol (CIPS) 対応インターフェイスを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug cisp** [**all** | **errors** | **events** | **packets** | **sync**]

**no debug cisp** [**all** | **errors** | **events** | **packets** | **sync**]

## 構文の説明

|                |                                  |
|----------------|----------------------------------|
| <b>all</b>     | (任意) CISP デバッグ メッセージをすべて表示します。   |
| <b>errors</b>  | (任意) CISP デバッグ メッセージを表示します。      |
| <b>events</b>  | (任意) CISP イベント デバッグ メッセージを表示します。 |
| <b>packets</b> | (任意) CISP パケット デバッグ メッセージを表示します。 |
| <b>sync</b>    | (任意) CISP 操作同期デバッグ メッセージを表示します。  |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug cisp** コマンドは、**no debug cisp** コマンドと同じです。

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <b>cisp enable</b>  | Client Information Signalling Protocol (CISP) をイネーブルにします。 |
| <b>dot1x credentials</b> (グローバル コンフィギュレーション) <i>profile</i> | プロファイルをサブリカント スイッチに設定します。                                 |
| <b>show cisp</b>  | 指定されたインターフェイスの CISP 情報を表示します。                             |

# debug cluster

クラスタ固有イベントのデバッグをイネーブルにするには、特権 EXEC モードで **debug cluster** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug cluster {discovery | events | extended | hsrp | http | ip [packet] | members | nat | neighbors
| platform | snmp | vqpxy}
```

```
no debug cluster {discovery | events | extended | hsrp | http | ip [packet] | members | nat |
neighbors | platform | snmp | vqpxy}
```

## 構文の説明

|                  |  |
|------------------|--|
| <b>discovery</b> | クラスタ ディスカバリ デバッグ メッセージを表示します。                    |
| <b>events</b>    | クラスタ イベント デバッグ メッセージを表示します。                      |
| <b>extended</b>  | 拡張ディスカバリ デバッグ メッセージを表示します。                       |
| <b>hsrp</b>      | ホットスタンバイ ルータ プロトコル (HSRP) デバッグ メッセージを表示します。      |
| <b>http</b>      | ハイパーテキスト転送プロトコル (HTTP) デバッグ メッセージを表示します。         |
| <b>ip packet</b> | IP またはトランスポート パケット デバッグ メッセージを表示します。             |
| <b>members</b>   | クラスタ メンバ デバッグ メッセージを表示します。                       |
| <b>nat</b>       | ネットワーク アドレス変換 (NAT) デバッグ メッセージを表示します。            |
| <b>neighbors</b> | クラスタ ネイバー デバッグ メッセージを表示します。                      |
| <b>platform</b>  | プラットフォーム固有のクラスタ デバッグ メッセージを表示します。                |
| <b>snmp</b>      | 簡易ネットワーク管理プロトコル (SNMP) デバッグ メッセージを表示します。         |
| <b>vqpxy</b>     | VLAN Query Protocol (VQP) プロキシ デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でだけ使用できます。

**undebug cluster** コマンドは、**no debug cluster** コマンドと同じです。

## 関連コマンド

| コマンド                           | 説明  |
|--------------------------------|---|
| <b>show debugging</b>          | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show cluster</b>            | スイッチが属するクラスタのステータスおよびサマリーを表示します。  |
| <b>show cluster candidates</b> | コマンド スイッチ上で入力された場合に候補スイッチのリストを表示します。  |
| <b>show cluster members</b>    | コマンド スイッチ上で実行された場合にクラスタ メンバに関する情報を表示します。  |

# debug dot1x

IEEE 802.1x 認証機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug dot1x** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug dot1x {all | errors | events | feature | packets | registry | state-machine}**

**no debug dot1x {all | errors | events | feature | packets | registry | state-machine}**

## 構文の説明

|                      |   |
|----------------------|---|
| <b>all</b>           | すべての IEEE 802.1x 認証デバッグ メッセージを表示します。    |
| <b>errors</b>        | IEEE 802.1x エラー デバッグ メッセージを表示します。       |
| <b>events</b>        | IEEE 802.1x イベント デバッグ メッセージを表示します。      |
| <b>feature</b>       | IEEE 802.1x 機能のデバッグ メッセージを表示します。        |
| <b>packets</b>       | IEEE 802.1x パケット デバッグ メッセージを表示します。      |
| <b>registry</b>      | 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。 |
| <b>state-machine</b> | ステートマシン関連イベントのデバッグ メッセージをデバッグします。       |



(注)

**redundancy** 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show dot1x</b>     | スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。   |

# debug dtp

ダイナミック トランキンング プロトコル (DTP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug dtp** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug dtp** {aggregation | all | decision | events | oserrs | packets | queue | states | timers}

**no debug dtp** {aggregation | all | decision | events | oserrs | packets | queue | states | timers}

## 構文の説明

|                    |  |
|--------------------|--|
| <b>aggregation</b> | DTP ユーザ メッセージ アグリゲーション デバッグ メッセージを表示します。 |
| <b>all</b>         | すべての DTP デバッグ メッセージを表示します。               |
| <b>decision</b>    | DTP 決定テーブル デバッグ メッセージを表示します。             |
| <b>events</b>      | DTP イベント デバッグ メッセージを表示します。               |
| <b>oserrs</b>      | DTP オペレーティング システム関連エラー デバッグ メッセージを表示します。 |
| <b>packets</b>     | DTP パケット処理デバッグ メッセージを表示します。              |
| <b>queue</b>       | DTP パケット キューイング デバッグ メッセージを表示します。        |
| <b>states</b>      | DTP ステート遷移デバッグ メッセージを表示します。              |
| <b>timers</b>      | DTP タイマー イベント デバッグ メッセージを表示します。          |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug dtp** コマンドは、**no debug dtp** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show dtp</b>       | スイッチまたは指定されたインターフェイスの DTP 情報を表示します。   |

# debug eap

拡張認証プロトコル (EAP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug eap** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug dot1x {all | authenticator | errors | events | md5 | packets | peer | sm}
```

```
no debug dot1x {all | authenticator | errors | events | md5 | packets | peer | sm}
```

## 構文の説明

|                      |                                      |
|----------------------|--------------------------------------|
| <b>all</b>           | すべての EAP デバッグ メッセージを表示します。           |
| <b>authenticator</b> | オーセンティケータ デバッグ メッセージを表示します。          |
| <b>errors</b>        | EAP エラー デバッグ メッセージを表示します。            |
| <b>events</b>        | EAP イベント デバッグ メッセージを表示します。           |
| <b>md5</b>           | EAP-MD5 デバッグ メッセージを表示します。            |
| <b>packets</b>       | EAP パケットのデバッグ メッセージを表示します。           |
| <b>peer</b>          | EAP ピア デバッグ メッセージを表示します。             |
| <b>sm</b>            | EAP ステート マシン関連イベント デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show eap</b>       | スイッチまたは指定されたポートの EAP のレジストレーション情報およびセッション情報を表示します。  |

# debug etherchannel

EtherChannel/PAgP シムのデバッグをイネーブルにするには、特権 EXEC モードで **debug etherchannel** コマンドを使用します。このシムは、ポート集約プロトコル (PAgP) ソフトウェア モジュールとポート マネージャ ソフトウェア モジュール間のインターフェイスとなるソフトウェア モジュールです。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug etherchannel** [**all** | **detail** | **error** | **event** | **idb**]

**no debug etherchannel** [**all** | **detail** | **error** | **event** | **idb**]

## 構文の説明

|               |   |
|---------------|---|
| <b>all</b>    | (任意) EtherChannel デバッグ メッセージをすべて表示します。      |
| <b>detail</b> | (任意) 詳細な EtherChannel デバッグ メッセージを表示します。     |
| <b>error</b>  | (任意) EtherChannel エラー デバッグ メッセージを表示します。     |
| <b>event</b>  | (任意) 主な EtherChannel イベント メッセージをデバッグします。    |
| <b>idb</b>    | (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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|--------------------------|---|
| <b>show debugging</b>    | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show etherchannel</b> | チャンネルの EtherChannel 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、特権 EXEC モードで **debug interface** 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 : <b>gigabitethernet 0/2</b> ) によって識別される、指定された物理ポートのデバッグ メッセージをデバッグします。 |
| <b>null interface-number</b>                      | 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。<br><i>interface-number</i> は常に <b>0</b> です。                         |
| <b>port-channel</b><br><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> の範囲は 1 ~ 6 です。   |
| <b>vlan vlan-id</b>                               | 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|--------------------------|---|
| <b>show debugging</b>    | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show etherchannel</b> | チャネルの EtherChannel 情報を表示します。  |

# debug ip dhcp snooping

DHCP スヌーピングのデバッグをイネーブルにするには、特権 EXEC モードで **debug ip dhcp snooping** 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

|                    |   |
|--------------------|---|
| <b>mac-address</b> | 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。 |
| <b>agent</b>       | 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。          |
| <b>event</b>       | 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。            |
| <b>packet</b>      | DHCP スヌーピングのデバッグ メッセージを表示します。                 |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug ip verify source packet

IP ソース ガードのデバッグをイネーブルにするには、特権 EXEC モードで **debug ip verify source packet** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug ip verify source packet**

**no debug ip verify source packet**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug ip igmp filter

インターネット グループ管理プロトコル (IGMP) フィルタ イベントのデバッグをイネーブルにするには、特権 EXEC モードで **debug ip igmp filter** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug ip igmp filter**

**no debug ip igmp filter**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug ip igmp max-groups

インターネットグループ管理プロトコル (IGMP) の最大のグループ イベントのデバッグをイネーブルにするには、特権 EXEC モードで **debug ip igmp max-groups** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug ip igmp max-groups**

**no debug ip igmp max-groups**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug ip igmp snooping

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 アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug igmp snooping** 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

|                   |   |
|-------------------|---|
| <b>group</b>      | (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。 |
| <b>management</b> | (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。     |
| <b>querier</b>    | (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。         |
| <b>router</b>     | (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。  |
| <b>timer</b>      | (任意) IGMP スヌーピング タイマー イベントのデバッグ メッセージを表示します。    |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|---|---|
| <a href="#">debug platform ip igmp snooping</a> | 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。  |
| <a href="#">show debugging</a>                  | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug l2nat

設定を適用する際にリアルタイムでレイヤ 2 NAT の設定の詳細を表示するには、EXEC モードで **debug l2nat** 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** 形式を入力します。

```
debug l2nat { all | common | fpga }
```

```
no debug l2nat { all | common | fpga }
```

## 構文の説明

|               |   |
|---------------|---|
| <b>all</b>    | すべてのレイヤ 2 NAT 情報が含まれるデバッグ出力を表示します。      |
| <b>common</b> | 共通のレイヤ 2 NAT コードを含むデバッグ出力を表示します。        |
| <b>fpga</b>   | FPGA ドライバ レイヤ 2 NAT コードを含むデバッグ出力を表示します。 |

## コマンド デフォルト

なし

## コマンド モード

EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(2)EB | このコマンドが導入されました。 |

## 例

次に、すべてのリアルタイムのレイヤ 2 NAT 設定の詳細については、デバッグ出力をイネーブルにする例を示します。

```
Switch# debug l2nat all
```

次に、すべてのリアルタイムのレイヤ 2 NAT 設定の詳細については、デバッグ出力をディセーブルにする例を示します。

```
Switch# no debug l2nat all
```

## 関連コマンド

| コマンド  | 説明   |
|---|--|
| <a href="#">l2nat instance</a>                  | レイヤ 2 NAT インスタンスを作成するか、または特定のレイヤ 2 NAT インスタンスのサブモードを開始します。 |
| <a href="#">l2nat</a>                           | 選択したインターフェイスの 1 つまたはすべての VLAN にレイヤ 2 NAT インスタンスを適用します。     |
| <a href="#">show l2nat instance</a>             | 指定したレイヤ 2 NAT インスタンスの設定の詳細を表示します。                          |
| <a href="#">show l2nat interface</a>            | 1 つ以上のインターフェイスのレイヤ 2 NAT インスタンスの設定の詳細を表示します。               |
| <a href="#">show l2nat statistics</a>           | すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。                         |
| <a href="#">show l2nat statistics interface</a> | 指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。                         |

# debug lacp

Link Aggregation Control Protocol (LACP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug lacp** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug lacp** [**all** | **event** | **fsm** | **misc** | **packet**]

**no debug lacp** [**all** | **event** | **fsm** | **misc** | **packet**]

## 構文の説明

|               |  |
|---------------|--|
| <b>all</b>    | (任意) LACP デバッグ メッセージをすべて表示します。         |
| <b>event</b>  | (任意) LACP イベント デバッグ メッセージを表示します。       |
| <b>fsm</b>    | (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。 |
| <b>misc</b>   | (任意) 各種 LACP デバッグ メッセージを表示します。         |
| <b>packet</b> | (任意) LACP パケット デバッグ メッセージを表示します。       |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show lacp</b>      | LACP チャネル グループ情報を表示します。   |

# debug lldp packets

リンク層検出プロトコル (LLDP) パケットのデバッグをイネーブルにするには、特権 EXEC モードで **debug lldp packets** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug lldp packets**

**no debug lldp packets**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 lldp packets** コマンドは、**no debug lldp packets** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug mac-notification** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug mac-notification**

**no debug mac-notification**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|--|---|
| <b>show debugging</b>                      | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show mac address-table notification</b> | 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

プラットフォームに依存しない MAC アドレス管理のデバッグをイネーブルにするには、特権 EXEC モードで **debug matm** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug matm**

**no debug matm**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 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  |
|----------------------------|---|
| <b>debug platform matm</b> | 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。   |
| <b>show debugging</b>      | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug matm move update** コマンドを使用します。

**debug matm move update**

**no debug matm move update**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|---|---|
| <b>mac address-table move update</b> {receive   transmit} | スイッチに MAC アドレス テーブル移行更新機能を設定します。  |
| <b>show debugging</b>                                     | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show mac address-table move update</b>                 | 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

スイッチドポートアナライザ (SPAN) 機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug monitor** 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

|                      |  |
|----------------------|--|
| <b>all</b>           | すべての SPAN デバッグ メッセージを表示します。                        |
| <b>errors</b>        | 詳細 SPAN エラー デバッグ メッセージを表示します。                      |
| <b>idb-update</b>    | SPAN インターフェイス記述ブロック (IDB) 更新トレース デバッグ メッセージを表示します。 |
| <b>info</b>          | SPAN 情報追跡デバッグ メッセージを表示します。                         |
| <b>list</b>          | 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。            |
| <b>notifications</b> | SPAN 通知デバッグ メッセージを表示します。                           |
| <b>platform</b>      | 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。                   |
| <b>requests</b>      | SPAN 要求デバッグ メッセージを表示します。                           |
| <b>snmp</b>          | SPAN および簡易ネットワーク管理プロトコル (SNMP) 追跡デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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。

## ■ debug monitor

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show monitor</b>   | 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

マルチキャスト VLAN レジストレーション (MVR) のデバッグをイネーブルにするには、特権 EXEC モードで **debug mvrdbg** 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

|                   |   |
|-------------------|---|
| <b>all</b>        | すべての MVR アクティビティ デバッグ メッセージを表示します。                              |
| <b>events</b>     | MVR イベント処理デバッグ メッセージを表示します。                                     |
| <b>igmpsn</b>     | MVR 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 アクティビティ デバッグ メッセージを表示します。 |
| <b>management</b> | 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。                                 |
| <b>ports</b>      | MVR ポート デバッグ メッセージを表示します。                                       |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show mvr</b>       | 現在の MVR 設定を表示します。   |

# debug nmsp

スイッチのネットワーク モビリティ サービス プロトコル (NMSP) のデバッグをイネーブルにするには、特権 EXEC モードで **debug nmsp** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug nmsp {all | connection | error | event | packet | rx | tx}
```

```
no debug nmsp
```

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug nmsp** コマンドは、**no debug nmsp** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show nmsp</b>      | NMSP 情報を表示します。  |

# debug nvram

NVRAM アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug nvram** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug nvram**

**no debug nvram**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug pagp

ポート集約プロトコル (PAgP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug pagp** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug pagp** [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

**no debug pagp** [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

## 構文の説明

|                    |                                       |
|--------------------|---------------------------------------|
| <b>all</b>         | (任意) PAgP デバッグ メッセージをすべて表示します。        |
| <b>dual-active</b> | (任意) デュアルアクティブ検出メッセージを表示します。          |
| <b>event</b>       | (任意) PAgP イベント デバッグ メッセージを表示します。      |
| <b>fsm</b>         | (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。 |
| <b>misc</b>        | (任意) 各種 PAgP デバッグ メッセージを表示します。        |
| <b>packet</b>      | (任意) PAgP パケット デバッグ メッセージを表示します。      |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show pagp</b>      | PAgP チャネル グループ情報を表示します。   |

# debug platform acl

アクセス コントロール リスト (ACL) マネージャのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform acl** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug platform acl {all | exit | label | main | racl | vacl | vmap | warn}
```

```
no debug platform acl {all | exit | label | main | racl | vacl | vmap | warn}
```

## 構文の説明

|              |                                  |
|--------------|----------------------------------|
| <b>all</b>   | すべての ACL マネージャ デバッグ メッセージを表示します。 |
| <b>exit</b>  | ACL 終了関連デバッグ メッセージを表示します。        |
| <b>label</b> | ACL ラベル関連デバッグ メッセージを表示します。       |
| <b>main</b>  | 主な、または重要な ACL デバッグ メッセージを表示します。  |
| <b>racl</b>  | ルータ ACL 関連デバッグ メッセージを表示します。      |
| <b>vacl</b>  | VLAN ACL 関連デバッグ メッセージを表示します。     |
| <b>vmap</b>  | ACL VLAN マップ関連デバッグ メッセージを表示します。  |
| <b>warn</b>  | ACL 警告関連デバッグ メッセージを表示します。        |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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。



(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。

```
Switch# debug platform acl ?
all          ACL Manager All
exit         ACL Exit related events
expand      VMR L4Op allocation/expansion related events
fspan       ACL Fspan related events
ipe         ACL IPE related events
ipv6        ACL IPv6 related
label       ACL Label related events
limitations ACL Limitations related events
main        ACL Main related events
odm         ODM related events
port-acl    Port-ACL related events
racl        ACL Racl related events
stack       ACL Stack related events
urpf        ACL URPF related events
vacl        ACL Vacl related events
```

## ■ debug platform acl

```

vlmap      ACL Vlmap related events
warn       ACL Warn related events

```

```
Switch#
```

---

**関連コマンド**

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform backup interface** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug platform backup interface**

**no debug platform backup interface**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

プラットフォーム バックアップ インターフェイス デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 debug platform backup interface** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform cisp

1 つ以上の Client Information Signalling Protocol (CISP) 対応インターフェイスがあるスイッチのプラットフォーム レベルのデバッグをイネーブルにするには、グローバル コンフィギュレーション モードで **debug platform cisp** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug platform cisp** [initialization | interface-configuration | rpc]

**no debug platform cisp** [initialization | interface-configuration | rpc]

## 構文の説明

|                                |                                    |
|--------------------------------|------------------------------------|
| <b>initialization</b>          | (任意) CISP 初期化シーケンスのデバッグをイネーブルにします。 |
| <b>interface-configuration</b> | (任意) CISP 設定のデバッグをイネーブルにします。       |
| <b>rpc</b>                     | (任意) CISP RPC 要求のデバッグをイネーブルにします。   |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug platform cisp** コマンドは、**no debug platform cisp** コマンドと同じです。

## 関連コマンド

| コマンド  | 説明  |
|---|---|
| <b>cisp enable</b>  | Client Information Signalling Protocol (CISP) をイネーブルにします。 |
| <b>dot1x credentials</b> (グローバル コンフィギュレーション) <i>profile</i> | プロファイルをサブリカント スイッチに設定します。                                 |
| <b>show cisp</b>  | 指定されたインターフェイスの CISP 情報を表示します。                             |

# debug platform 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、特権 EXEC モードで **debug platform cpu-queues** 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

|                           |  |
|---------------------------|--|
| <b>broadcast-q</b>        | 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。   |
| <b>cbt-to-spt-q</b>       | 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。 |
| <b>cpuhub-q</b>           | 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。   |
| <b>host-q</b>             | 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。  |
| <b>icmp-q</b>             | インターネット制御メッセージプロトコル (ICMP) 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。                         |
| <b>igmp-snooping-q</b>    | 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 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。                  |
| <b>layer2-protocol-q</b>  | 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。  |
| <b>logging-q</b>          | 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。   |
| <b>remote-console-q</b>   | 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。   |
| <b>routing-protocol-q</b> | 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。  |
| <b>rpffail-q</b>          | リバース パス転送 (RPF) 障害キューによって受信されたパケットに関するデバッグ メッセージを表示します。                                  |
| <b>software-fwd-q</b>     | ソフトウェア転送キューによって受信されたパケットが受信した表示デバッグパケットのデバッグを表示します。                                      |
| <b>stp-q</b>              | スパニングツリー プロトコル (STP) キューによって受信されたパケットのデバッグを表示します。  |

## 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 cpu-queues

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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 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  |
|--------|-----------------------|---|
|        | <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform dot1x** 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

|                                |   |
|--------------------------------|---|
| <b>initialization</b>          | IEEE 802.1x 認証初期化シーケンス デバッグ メッセージを表示します。              |
| <b>interface-configuration</b> | 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。   |
| <b>rpc</b>                     | IEEE 802.1x リモート プロシージャ コール (RPC) 要求デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform etherchannel** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug platform etherchannel {init | link-up | rpc | warnings}
```

```
no debug platform etherchannel {init | link-up | rpc | warnings}
```

## 構文の説明

|                 |  |
|-----------------|--|
| <b>init</b>     | EtherChannel モジュール初期化デバッグ メッセージを表示します。               |
| <b>link-up</b>  | 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。   |
| <b>rpc</b>      | EtherChannel リモート プロシージャ コール (RPC) デバッグ メッセージを表示します。 |
| <b>warnings</b> | EtherChannel 警告デバッグ メッセージを表示します。                     |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform forw-tcam** 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

|                   |                                      |
|-------------------|--------------------------------------|
| <b>adjustment</b> | (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。   |
| <b>allocate</b>   | (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。 |
| <b>audit</b>      | (任意) TCAM マネージャ監査メッセージを表示します。        |
| <b>error</b>      | (任意) TCAM マネージャ エラー メッセージを表示します。     |
| <b>move</b>       | (任意) TCAM マネージャ移行メッセージを表示します。        |
| <b>read</b>       | (任意) TCAM マネージャ読み込みメッセージを表示します。      |
| <b>write</b>      | (任意) TCAM マネージャ書き込みメッセージを表示します。      |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform ip arp inspection

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 イベントをデバッグするには、特権 EXEC モードで **debug platform ip arp inspection** 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

|               |   |
|---------------|---|
| <b>all</b>    | すべてのダイナミック ARP インスペクション デバッグ メッセージを表示します。                     |
| <b>error</b>  | ダイナミック ARP インスペクション エラー デバッグ メッセージを表示します。                     |
| <b>event</b>  | ダイナミック ARP インスペクション イベント デバッグ メッセージを表示します。                    |
| <b>packet</b> | ダイナミック ARP インスペクション パケット関連デバッグ メッセージを表示します。                   |
| <b>rpc</b>    | ダイナミック ARP インスペクション リモート プロシージャ コール (RPC) 要求デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug platform ip arp inspection** コマンドは、**no debug platform ip arp inspection** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明   |
|-----------------------|--|
| <b>show inventory</b> | ダイナミック ARP インスペクションの設定および動作ステータスを表示します。  |
| <b>show debugging</b> | 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。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# debug platform ip dhcp

DHCP イベントをデバッグするには、特権 EXEC モードで **debug platform ip dhcp** 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

|               |   |
|---------------|---|
| <b>all</b>    | (任意) DHCP デバッグ メッセージをすべて表示します。                      |
| <b>error</b>  | (任意) DHCP エラー デバッグ メッセージを表示します。                     |
| <b>event</b>  | (任意) DHCP イベント デバッグ メッセージを表示します。                    |
| <b>packet</b> | (任意) DHCP パケット関連デバッグ メッセージを表示します。                   |
| <b>rpc</b>    | (任意) DHCP リモート プロシージャ コール (RPC) 要求デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|--------------------------------------|---|
| <b>show ip dhcp snooping</b>         | DHCP スヌーピング設定を表示します。  |
| <b>show ip dhcp snooping binding</b> | DHCP スヌーピング バインディング情報を表示します。  |
| <b>show debugging</b>                | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform ip igmp snooping

プラットフォームに依存するインターネットグループ管理プロトコル (IGMP) スヌーピングのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform ip igmp snooping** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug platform ip igmp snooping {all | di | error | event | group | mgmt | pak | retry | rpc | warn}
```

```
debug platform ip igmp snooping pak {ip-address | error | ipopt | leave | query | report | rx | svi | tx}
```

```
debug platform ip igmp snooping rpc [cfg | l3mm | misc | vlan]
```

```
no debug platform ip igmp snooping {all | di | error | event | group | mgmt | pak | retry | rpc | warn}
```

## 構文の説明

|   |   |
|---|---|
| <b>all</b>  | 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。  |
| <b>di</b>   | IGMP スヌーピング宛先インデックス (di) 調整リモート プロシージャ コール (RPC) デバッグ メッセージを表示します。  |
| <b>error</b>  | IGMP スヌーピング エラー メッセージを表示します。  |
| <b>event</b>  | 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。  |
| <b>group</b>  | 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。  |
| <b>mgmt</b>   | IGMP スヌーピング管理デバッグ メッセージを表示します。  |
| <b>pak</b> { <i>ip-address</i>   <b>error</b>   <b>ipopt</b>   <b>leave</b>   <b>query</b>   <b>report</b>   <b>rx</b>   <b>svi</b>   <b>tx</b> } | <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"> <li>• <b>ip-address</b> : IGMP グループの IP アドレス</li> <li>• <b>error</b> : 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。</li> <li>• <b>ipopt</b> : 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。</li> <li>• <b>leave</b> : IGMP スヌーピング脱退デバッグ メッセージを表示します。</li> <li>• <b>query</b> : 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。</li> <li>• <b>report</b> : 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。</li> <li>• <b>rx</b> : 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。</li> <li>• <b>svi</b> : IGMP スヌーピング スイッチ仮想インターフェイス (SVI) パケット デバッグ メッセージを表示します。</li> <li>• <b>tx</b> : 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。</li> </ul> |
| <b>retry</b>  | 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。  |

|                                       |   |
|---------------------------------------|---|
| <b>rpc [cfg   l3mm   misc   vlan]</b> | IGMP スヌーピング リモート プロシージャ コール (RPC) イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>cfg</b> : (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。</li> <li>• <b>l3mm</b> : (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。</li> <li>• <b>misc</b> : (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。</li> <li>• <b>vlan</b> : (任意) IGMP スヌーピング VLAN アサート RPC デバッグ メッセージを表示します。</li> </ul> |
| <b>warn</b>                           | IGMP スヌーピング警告メッセージを表示します。   |

**デフォルト** デバッグはディセーブルです。

**コマンド モード** 特権 EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが追加されました。 |

**使用上のガイドライン** **undebug platform ip igmp snooping** コマンドは、**no debug platform ip igmp snooping** コマンドと同じです。

| 関連コマンド | コマンド                          | 説明  |
|--------|-------------------------------|---|
|        | <b>debug ip igmp snooping</b> | 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。   |
|        | <b>show debugging</b>         | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform ip source-guard

IP ソース ガード イベントをデバッグするには、特権 EXEC モードで **debug platform ip source-guard** 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

|              |   |
|--------------|---|
| <b>all</b>   | 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。 |
| <b>error</b> | 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。  |
| <b>event</b> | IP 送信元ガード プラットフォーム イベント デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|---------------------------------------|---|
| <a href="#">show ip verify source</a> | IP 送信元ガードの設定を表示します。   |
| <b>show debugging</b>                 | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform ip unicast

プラットフォームに依存する IP ユニキャストのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform ip unicast** 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}
```



(注) このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

## 構文の説明

|                   |   |
|-------------------|---|
| <b>adjacency</b>  | 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。  |
| <b>all</b>        | 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。<br><br>(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。   |
| <b>arp</b>        | IP ユニキャスト ルーティングのアドレス解決プロトコル (ARP) 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。                                  |
| <b>dhcp</b>       | 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。   |
| <b>errors</b>     | 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。   |
| <b>events</b>     | 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。                                     |
| <b>interface</b>  | 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。  |
| <b>mpath</b>      | 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。                   |
| <b>registries</b> | IP ユニキャスト ルーティング転送情報データベース (FIB)、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。                           |
| <b>retry</b>      | 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。 |
| <b>route</b>      | 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。  |
| <b>rpc</b>        | IP ユニキャスト ルーティング レイヤ 3 ユニキャストリモート プロシージャ コール (RPC) 相互作用のデバッグ メッセージを表示します。                             |
| <b>standby</b>    | ホットスタンバイ ルータ プロトコル (HSRP) の問題発生時のトラブルシューティングに役立つ、IP ユニキャスト ルーティング スタンバイ イベントのデバッグ メッセージを表示します。        |
| <b>statistics</b> | 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。  |

## ■ debug platform ip unicast

**デフォルト** デバッグはディセーブルです。

**コマンドモード** 特権 EXEC

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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 ip unicast` コマンドは、`no debug platform ip unicast` コマンドと同じです。

**例** 次に、すべてのプラットフォームの IP ユニキャスト ルーティングをオンにする例を示します。

```
Switch# debug platform ip unicast all
debug platform ip-unicast all debugging is on
Switch#
```

次に、すべてのプラットフォームの IP ユニキャスト ルーティングをオフにする例を示します。

```
Switch# undebbug platform ip unicast all
debug platform ip-unicast all debugging is off
Switch#
```

# debug platform led

発光ダイオード（LED）動作のデバッグをイネーブルにするには、特権 EXEC モードで **debug platform led** 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

|                |                                 |
|----------------|---------------------------------|
| <b>generic</b> | LED 総称アクション デバッグ メッセージを表示します。   |
| <b>signal</b>  | 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform matm** 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

|                       |   |
|-----------------------|---|
| <b>aging</b>          | 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。                    |
| <b>all</b>            | 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。       |
| <b>ec-aging</b>       | 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。          |
| <b>errors</b>         | MAC アドレス管理エラー メッセージを表示します。                          |
| <b>learning</b>       | MAC アドレス管理アドレス学習デバッグ メッセージを表示します。                   |
| <b>rpc</b>            | MAC アドレス管理リモート プロシージャ コール (RPC) 関連デバッグ メッセージを表示します。 |
| <b>secure-address</b> | MAC アドレス管理セキュア アドレス学習デバッグ メッセージを表示します。              |
| <b>warning</b>        | MAC アドレス管理警告メッセージを表示します。                            |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug platform matm** コマンドは、**no debug platform matm** コマンドと同じです。

## 関連コマンド

| コマンド                           | 説明  |
|--------------------------------|---|
| <a href="#">debug matm</a>     | 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。  |
| <a href="#">show debugging</a> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform messaging application** 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

|                 |  |
|-----------------|--|
| <b>all</b>      | 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。 |
| <b>badpak</b>   | 不良パケット デバッグ メッセージを表示します。               |
| <b>cleanup</b>  | クリーンアップ デバッグ メッセージを表示します。              |
| <b>events</b>   | イベント デバッグ メッセージを表示します。                 |
| <b>memerr</b>   | メモリ エラー デバッグ メッセージを表示します。              |
| <b>messages</b> | 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。     |
| <b>usererr</b>  | 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug platform messaging application** コマンドは、**no debug platform messaging application** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明   |
|-----------------------|--|
| <b>show debugging</b> | 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。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# 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、特権 EXEC モードで **debug platform phy** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug platform phy {automdix | cablediag | dual-purpose | flcd {configure | ipc | iter | trace} |
  flowcontrol | forced | init-seq | link-status | read | sfp | show-controller | speed | write |
  xenpak}
```

```
no debug platform phy {automdix | cablediag | dual-purpose | flcd {configure | ipc | iter | trace} |
  flowcontrol | forced | init-seq | link-status | read | sfp | show-controller | speed | write |
  xenpak}
```

## 構文の説明

|  |   |
|--|---|
| <b>automdix</b>                              | PHY Automatic Medium-Dependent Interface Crossover (Auto-MDIX) デバッグ メッセージを表示します。  |
| <b>cablediag</b>                             | PHY ケーブル診断デバッグ メッセージを表示します。   |
| <b>dual-purpose</b>                          | PHY デュアルパーパス イベント デバッグ メッセージを表示します。   |
| <b>flcd {configure   ipc   iter   trace}</b> | 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"> <li><b>configure</b> : PHY 設定デバッグ メッセージを表示します。</li> <li><b>ipc</b> : プロセス間通信プロトコル (IPC) のデバッグ メッセージを表示します。</li> <li><b>iter</b> : iter デバッグ メッセージを表示します。</li> <li><b>trace</b> : トレースのデバッグ メッセージを表示します。</li> </ul> |
| <b>flowcontrol</b>                           | PHY フロー制御デバッグ メッセージを表示します。  |
| <b>forced</b>                                | PHY 強制モードデバッグ メッセージを表示します。  |
| <b>init-seq</b>                              | PHY 初期化シーケンス デバッグ メッセージを表示します。  |
| <b>link-status</b>                           | PHY リンク ステータス デバッグ メッセージを表示します。   |
| <b>read</b>                                  | PHY-read デバッグ メッセージを表示します。  |
| <b>sfp</b>                                   | Small Form-Factor Pluggable (SFP) モジュール デバッグ メッセージを表示します。   |
| <b>show-controller</b>                       | PHY show controller デバッグ メッセージを表示します。   |
| <b>speed</b>                                 | PHY 速度変更デバッグ メッセージを表示します。   |
| <b>write</b>                                 | PHY-write デバッグ メッセージを表示します。   |
| <b>xenpak</b>                                | PHY XENPAK デバッグ メッセージを表示します。  |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform pm** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug platform pm {all | counters | errdisable | etherchnl | exceptions | hpm-events | idb-events
| if-numbers | ios-events | link-status | platform | pm-events | pm-span | pm-vectors [detail]
| rpc [general | oper-info | state | vectors | vp-events] | soutput-vectors | sync | vlans}
```

```
no debug platform pm {all | counters | errdisable | etherchnl | exceptions | hpm-events |
idb-events | if-numbers | ios-events | link-status | platform | pm-events | pm-span |
pm-vectors [detail] | rpc [general | oper-info | state | vectors | vp-events] | soutput-vectors |
sync | vlans}
```

## 構文の説明

|  |  |
|--|--|
| <b>all</b>   | 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。  |
| <b>counters</b>  | リモート プロシージャ コール (RPC) デバッグ メッセージのカウントを表示します。   |
| <b>errdisable</b>  | エラー ディセーブル関連イベント デバッグ メッセージを表示します。   |
| <b>etherchnl</b>   | EtherChannel 関連イベント デバッグ メッセージを表示します。  |
| <b>exceptions</b>  | システム例外デバッグ メッセージを表示します。  |
| <b>hpm-events</b>  | 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。  |
| <b>idb-events</b>  | 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。  |
| <b>if-numbers</b>  | インターフェイス番号の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。  |
| <b>ios-events</b>  | Cisco IOS イベント デバッグ メッセージを表示します。   |
| <b>link-status</b>   | 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。   |
| <b>platform</b>  | 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。  |
| <b>pm-events</b>   | 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。   |
| <b>pm-span</b>   | ポート マネージャ スイッチド ポート アナライザ (SPAN) イベント デバッグ メッセージを表示します。  |
| <b>pm-vectors [detail]</b>                                     | 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"> <li>• <b>detail</b> : ベクトル機能の詳細を表示します。</li> </ul>  |
| <b>rpc [general   oper-info   state   vectors   vp-events]</b> | 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"> <li>• <b>general</b> : (任意) RPC 一般イベントを表示します。</li> <li>• <b>oper-info</b> : (任意) 操作および情報関連 RPC メッセージを表示します。</li> <li>• <b>state</b> : (任意) 管理および操作関連 RPC メッセージを表示します。</li> <li>• <b>vectors</b> : (任意) ベクタ関連 RPC メッセージを表示します。</li> <li>• <b>vp-events</b> : (任意) 仮想ポート関連イベント RP メッセージを表示します。</li> </ul> |
| <b>soutput-vectors</b>   | 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。   |

|             |   |
|-------------|---|
| <b>sync</b> | 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。 |
| <b>vlan</b> | 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

| コマンド履歴 | リリース      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが追加されました。 |

**使用上のガイドライン** **undebug platform pm** コマンドは、**no debug platform pm** コマンドと同じです。

| 関連コマンド | コマンド                  | 説明  |
|--------|-----------------------|---|
|        | <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform port-asic

ポート特定用途向け集積回路（ASIC）ドライバのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform port-asic** 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

|                  |                                    |
|------------------|------------------------------------|
| <b>interrupt</b> | 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。 |
| <b>periodic</b>  | 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。 |
| <b>read</b>      | ポート ASIC 読み取りデバッグ メッセージを表示します。     |
| <b>write</b>     | ポート ASIC 書き込みデバッグ 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform port-security** 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

|                 |                                       |
|-----------------|---------------------------------------|
| <b>add</b>      | 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。           |
| <b>aging</b>    | 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。      |
| <b>all</b>      | すべてのポート セキュリティのデバッグ メッセージを表示します。      |
| <b>delete</b>   | 表示セキュア アドレス削除デバッグ メッセージを表示します。        |
| <b>errors</b>   | 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。      |
| <b>rpc</b>      | リモートプロシージャコール (RPC) デバッグ メッセージを表示します。 |
| <b>warnings</b> | 警告デバッグ メッセージを表示します。                   |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform qos-acl-tcam

Quality of Service (QoS) およびアクセス コントロール リスト (ACL) 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、特権 EXEC モードで **debug platform qos-acl-tcam** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | rpc | tcam}
```

```
no debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | rpc | tcam}
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|               |  |
|---------------|--|
| <b>all</b>    | 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。 |
| <b>ctcam</b>  | Cisco TCAM (CTCAM) 関連イベント デバッグ メッセージを表示します。          |
| <b>errors</b> | 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。                     |
| <b>labels</b> | 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。                     |
| <b>mask</b>   | 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。                     |
| <b>rpc</b>    | QATM リモート プロシージャ コール (RPC) 関連イベント デバッグ メッセージを表示します。  |
| <b>tcam</b>   | QATM TCAM 関連イベント デバッグ メッセージを表示します。                   |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform resource-manager** 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

|               |  |
|---------------|--|
| <b>all</b>    | 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。                       |
| <b>dm</b>     | 宛先マップ デバッグ メッセージを表示します。                                |
| <b>erd</b>    | 等コスト 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。                      |
| <b>errors</b> | エラー デバッグ メッセージを表示します。                                  |
| <b>madmed</b> | 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。 |
| <b>sd</b>     | 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。                        |
| <b>stats</b>  | 統計デバッグ メッセージを表示します。                                    |
| <b>vld</b>    | VLAN リスト記述子デバッグ メッセージを表示します。                           |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug platform resource-manager** コマンドは、**no debug platform resource-manager** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform snmp

プラットフォームに依存する簡易ネットワーク管理プロトコル (SNMP) ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform snmp** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug platform snmp**

**no debug platform snmp**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform span

プラットフォームに依存するスイッチド ポート アナライザ (SPAN) ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform span** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug platform span**

**no debug platform span**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform supervisor-asic

スーパーバイザ特定用途向け集積回路（ASIC）のデバッグをイネーブルにするには、特権 EXEC モードで **debug platform supervisor-asic** 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

|                |   |
|----------------|---|
| <b>all</b>     | 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。 |
| <b>errors</b>  | 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。      |
| <b>receive</b> | 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。        |
| <b>send</b>    | スーパーバイザ ASIC 送信デバッグ メッセージを表示します。        |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug platform supervisor-asic** コマンドは、**no debug platform supervisor-asic** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform sw-bridge

ソフトウェアブリッジ機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug platform sw-bridge** 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

|                  |                                |
|------------------|--------------------------------|
| <b>broadcast</b> | 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。 |
| <b>control</b>   | プロトコル パケット デバッグ メッセージを表示します。   |
| <b>multicast</b> | 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。  |
| <b>packet</b>    | 送受信データ デバッグ メッセージを表示します。       |
| <b>unicast</b>   | ユニキャスト データ デバッグ メッセージを表示します。   |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug platform tcam** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```

debug platform tcam {log | read | search | write}
debug platform tcam log l2 {acl {input | output} | local | qos}
debug platform tcam log l3 {acl {input | output} | ipv6 {acl {input | output} | local | qos |
secondary} | local | qos | secondary}
debug platform tcam read {reg | ssram | tcam}
debug platform tcam search
debug platform tcam write {forw-ram | reg | tcam}
no debug platform tcam {log | read | search | write}
no debug platform tcam log l2 {acl {input | output} | local | qos}
no debug platform tcam log l3 {acl {input | output} | ipv6 {acl {input | output} | local | qos |
secondary} | local | qos | secondary}
no debug platform tcam read {reg | ssram | tcam}
no debug platform tcam search
no debug platform tcam write {forw-ram | reg | tcam}

```

## 構文の説明

|  |  |
|--|--|
| <b>log l2 {acl {input   output}   local   qos}</b> | 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"> <li>• <b>acl {input   output}</b>: 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。</li> <li>• <b>local</b>: 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。</li> <li>• <b>qos</b>: 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。</li> </ul> |
|--|--|

|  |  |
|--|--|
| <b>l3 {acl {input   output}   ipv6 {acl {input   output}   local   qos   secondary}   local   qos   secondary}</b> | 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"> <li>• <b>acl {input   output}</b>: 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。</li> <li>• <b>ipv6 {acl {input   output}   local   qos   secondary}</b>: IPv6 ベース ルックアップ デバッグ メッセージを表示します。オプションには、入力または出力 ACL ルックアップ、ローカル フォワーディング ルックアップ、および QoS ルックアップ、またはセカンダリ フォワーディング ルックアップ デバッグ メッセージの表示が含まれます。</li> <li>• <b>local</b>: 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。</li> <li>• <b>qos</b>: 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。</li> <li>• <b>secondary</b>: 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。</li> </ul> |
| <b>read {reg   ssram   tcam}</b>   | TCAM-read 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"> <li>• <b>reg</b>: TCAM レジスタ読み取りデバッグ メッセージを表示します。</li> <li>• <b>ssram</b>: Synchronous Static RAM (SSRAM) 読み取りデバッグ メッセージを表示します。</li> <li>• <b>tcam</b>: TCAM 読み取りデバッグ メッセージを表示します。</li> </ul>   |
| <b>search</b>  | 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。  |
| <b>write {forw-ram   reg   tcam}</b>   | TCAM-write 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><b>forw-ram</b>: 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><b>reg</b>: 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><b>tcam</b>: TCAM 書き込みデバッグ メッセージを表示します。</p>  |

**デフォルト**

デバッグはディセーブルです。

**コマンド モード**

特権 EXEC

**コマンド履歴**

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

**使用上のガイドライン****undebug platform tcam** コマンドは、**no debug platform tcam** コマンドと同じです。

## ■ debug platform tcam

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug platform udlld

プラットフォームに依存する単方向リンク検出 (UDLD) ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform udlld** 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 udlld [all | error | rpc {events | messages}]**

**no debug platform udlld [all | error | rpc {events | messages}]**

## 構文の説明

|                                |  |
|--------------------------------|--|
| <b>all</b>                     | (任意) UDLD デバッグ メッセージをすべて表示します。   |
| <b>error</b>                   | (任意) エラー条件デバッグ メッセージを表示します。  |
| <b>rpc {events   messages}</b> | (任意) UDLD リモート プロシージャ コール (RPC) デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>events</b> : UDLD RPC イベントを表示します。</li> <li><b>messages</b> : UDLD RPC メッセージを表示します。</li> </ul> |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 udlld** コマンドは、**no debug platform udlld** コマンドと同じです。

## 関連コマンド

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、EXEC モードで **debug platform vlan** 特権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

|               |  |
|---------------|--|
| <b>errors</b> | VLAN エラー デバッグ メッセージを表示します。                     |
| <b>mvid</b>   | 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。 |
| <b>rpc</b>    | リモート プロシージャ コール (RPC) デバッグ メッセージを表示します。        |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# debug pm

ポート マネージャ (PM) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug pm** 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 や単方向リンク検出 (UDLD) などを含むすべての機能は、ポート マネージャと連携して、スイッチに機能を提供します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug pm {all | assert | card | etherchnl | hatable | messages | port | redundancy | registry | sm |
span | split | vlan | vp}
```

```
no debug pm {all | assert | card | etherchnl | hatable | messages | port | redundancy | registry |
sm | span | split | vlan | vp}
```

## 構文の説明

|                   |  |
|-------------------|--|
| <b>all</b>        | すべての PM デバッグ メッセージを表示します。                |
| <b>assert</b>     | アサート デバッグ メッセージを表示します。                   |
| <b>card</b>       | 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。           |
| <b>etherchnl</b>  | EtherChannel 関連イベント デバッグ メッセージを表示します。    |
| <b>hatable</b>    | Host Access Table イベント デバッグ メッセージを表示します。 |
| <b>messages</b>   | PM デバッグ メッセージを表示します。                     |
| <b>port</b>       | ポート関連イベント デバッグ メッセージを表示します。              |
| <b>redundancy</b> | 冗長デバッグ メッセージを表示します。                      |
| <b>registry</b>   | 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。            |
| <b>sm</b>         | ステートマシン関連イベントのデバッグ メッセージをデバッグします。        |
| <b>span</b>       | 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。         |
| <b>split</b>      | 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。             |
| <b>vlan</b>       | VLAN 関連イベント デバッグ メッセージを表示します。            |
| <b>vp</b>         | 仮想ポート関連イベント デバッグ メッセージを表示します。            |



(注) **scp** および **pvlan** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## ■ debug pm

---

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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |

# 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、特権 EXEC モードで **debug port-security** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug port-security**

**no debug port-security**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|---------------------------|---|
| <b>show debugging</b>     | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show port-security</b> | 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 profinet alarm

PROFINET アラームのデバッグをイネーブルにするには、特権 EXEC モードで **debug profinet alarm** コマンドを使用します。PROFINET 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 profinet alarm**

**no debug profinet alarm**

## 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

PROFINET デバッグは設定されていません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**debug profinet alarm** コマンドは、**no debug profinet alarm** コマンドと同じです。

シスコのテクニカル サポート エンジニアの指示を受けた場合にのみ、このコマンドを使用してください。

このコマンドを使用する場合、シリアル ポート経由ではなく、イーサネット ポート経由で Telnet を使用して Cisco IOS ソフトウェアのコマンドライン インターフェイス (CLI) にアクセスします。

## 例

次の例では、PROFINET アラームのデバッグをイネーブルにする方法を示します。

```
Switch# debug profinet alarm
```

## 関連コマンド

| コマンド                           | 説明   |
|--------------------------------|--|
| <b>debug profinet cyclic</b>   | PROFINET 巡回パケットの送受信に関連するファンクション コールを表示します。       |
| <b>debug profinet error</b>    | PROFINET セッション エラーのデバッグをイネーブルにします。               |
| <b>debug profinet packet</b>   | PROFINET パケットのデバッグをイネーブルにします。                    |
| <b>debug profinet platform</b> | Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにします。 |
| <b>debug profinet topology</b> | 受信した PROFINET トポロジ パケットを表示します。                   |
| <b>debug profinet trace</b>    | トレースした一連のデバッグ出力ログを表示します。                         |
| <b>profinet</b>                | スイッチの PROFINET 機能をイネーブルにします。                     |

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show profinet</b>  | スイッチの PROFINET セッションの詳細を表示します。  |

# debug profinet cyclic

PROFINET 巡回パケットの送受信に関連するファンクション コールを表示するには、特権 EXEC モードで **debug profinet cyclic** コマンドを使用します。PROFINET 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 profinet cyclic**

**no debug profinet cyclic**

## 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

PROFINET デバッグは設定されていません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**undebug profinet cyclic** コマンドは、**no debug profinet cyclic** コマンドと同じです。

シスコのテクニカル サポート エンジニアの指示を受けた場合にのみ、このコマンドを使用してください。

このコマンドを使用する場合、シリアル ポート経由ではなく、イーサネット ポート経由で Telnet を使用して Cisco IOS ソフトウェアのコマンドライン インターフェイス (CLI) にアクセスします。

## 例

次の例では、タイム サイクル ベースの PROFINET イーサネット フレームに関する情報を表示する方法を示します。

```
Switch# debug profinet cyclic
```

## 関連コマンド

| コマンド                                    | 説明   |
|---|--|
| <a href="#">debug profinet alarm</a>    | PROFINET アラームのデバッグをイネーブルにします。                    |
| <a href="#">debug profinet error</a>    | PROFINET セッション エラーのデバッグをイネーブルにします。               |
| <a href="#">debug profinet packet</a>   | PROFINET パケットのデバッグをイネーブルにします。                    |
| <a href="#">debug profinet platform</a> | Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにします。 |
| <a href="#">debug profinet topology</a> | 受信した PROFINET トポロジ パケットを表示します。                   |
| <a href="#">debug profinet trace</a>    | トレースした一連のデバッグ出力ログを表示します。                         |
| <a href="#">profinet</a>                | スイッチの PROFINET 機能をイネーブルにします。                     |

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show profinet</b>  | スイッチの PROFINET セッションの詳細を表示します。  |

# debug profinet error

PROFINET セッション エラーのデバッグをイネーブルにするには、特権 EXEC モードで **debug profinet error** コマンドを使用します。PROFINET 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 profinet error**

**no debug profinet error**

## 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

PROFINET デバッグは設定されていません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**undebug profinet error** コマンドは、**no debug profinet error** コマンドと同じです。

シスコのテクニカル サポート エンジニアの指示を受けた場合にのみ、このコマンドを使用してください。

このコマンドを使用する場合、シリアル ポート経由ではなく、イーサネット ポート経由で Telnet を使用して Cisco IOS ソフトウェアのコマンドライン インターフェイス (CLI) にアクセスします。

## 例

次の例では、PROFINET エラーのデバッグをイネーブルにする方法を示します。

```
Switch# debug profinet error
```

## 関連コマンド

| コマンド                           | 説明   |
|--------------------------------|--|
| <b>debug profinet alarm</b>    | PROFINET アラームのデバッグをイネーブルにします。                    |
| <b>debug profinet cyclic</b>   | PROFINET 巡回パケットの送受信に関連するファンクション コールを表示します。       |
| <b>debug profinet packet</b>   | PROFINET パケットのデバッグをイネーブルにします。                    |
| <b>debug profinet platform</b> | Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにします。 |
| <b>debug profinet topology</b> | 受信した PROFINET トポロジ パケットを表示します。                   |
| <b>debug profinet trace</b>    | トレースした一連のデバッグ出力ログを表示します。                         |
| <b>profinet</b>                | スイッチの PROFINET 機能をイネーブルにします。                     |

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show profinet</b>  | スイッチの PROFINET セッションの詳細を表示します。  |

# debug profinet packet

PROFINET 機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug profinet packet** コマンドを使用します。PROFINET 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 profinet packet {ethernet | udp}**

**no debug profinet packet {ethernet | udp}**

## 構文の説明

|                 |                                      |
|-----------------|--------------------------------------|
| <b>ethernet</b> | PROFINET イーサネット パケットのデバッグをイネーブルにします。 |
| <b>udp</b>      | PROFINET UDP パケットのデバッグをイネーブルにします。    |

## デフォルト

PROFINET デバッグは設定されていません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**undebug profinet packet** コマンドは、**no debug profinet packet** コマンドと同じです。

シスコのテクニカル サポート エンジニアの指示を受けた場合にのみ、このコマンドを使用してください。

このコマンドを使用する場合、シリアル ポート経由ではなく、イーサネット ポート経由で Telnet を使用して Cisco IOS ソフトウェアのコマンドライン インターフェイス (CLI) にアクセスします。

## 例

次の例では、PROFINET イーサネット パケットのデバッグをイネーブルにする方法を示します。

```
Switch# debug profinet packet ethernet
```

## 関連コマンド

| コマンド                                    | 説明   |
|---|--|
| <a href="#">debug profinet alarm</a>    | PROFINET アラームのデバッグをイネーブルにします。                    |
| <a href="#">debug profinet cyclic</a>   | PROFINET 巡回パケットの送受信に関連するファンクション コールを表示します。       |
| <a href="#">debug profinet error</a>    | PROFINET セッション エラーのデバッグをイネーブルにします。               |
| <a href="#">debug profinet platform</a> | Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにします。 |
| <a href="#">debug profinet topology</a> | 受信した PROFINET トポロジ パケットを表示します。                   |
| <a href="#">debug profinet trace</a>    | トレースした一連のデバッグ出力ログを表示します。                         |
| <a href="#">profinet</a>                | スイッチの PROFINET 機能をイネーブルにします。                     |

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show profinet</b>  | スイッチの PROFINET セッションの詳細を表示します。  |

# debug profinet platform

Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにするには、特権 EXEC モードで **debug profinet platform** コマンドを使用します。PROFINET 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 profinet platform**

**no debug profinet platform**

## 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

PROFINET デバッグは設定されていません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**undebug profinet platform** コマンドは、**no debug profinet platform** コマンドと同じです。

シスコのテクニカル サポート エンジニアの指示を受けた場合にのみ、このコマンドを使用してください。

このコマンドを使用する場合、シリアル ポート経由ではなく、イーサネット ポート経由で Telnet を使用して Cisco IOS ソフトウェアのコマンドライン インターフェイス (CLI) にアクセスします。

## 例

次の例では、Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにする方法を示します。

```
Switch# debug profinet platform
```

## 関連コマンド

| コマンド                                    | 説明   |
|---|--|
| <a href="#">debug profinet alarm</a>    | PROFINET アラームのデバッグをイネーブルにします。              |
| <a href="#">debug profinet cyclic</a>   | PROFINET 巡回パケットの送受信に関連するファンクション コールを表示します。 |
| <a href="#">debug profinet error</a>    | PROFINET セッション エラーのデバッグをイネーブルにします。         |
| <a href="#">debug profinet packet</a>   | PROFINET パケットのデバッグをイネーブルにします。              |
| <a href="#">debug profinet topology</a> | 受信した PROFINET トポロジ パケットを表示します。             |
| <a href="#">debug profinet trace</a>    | トレースした一連のデバッグ出力ログを表示します。                   |
| <a href="#">profinet</a>                | スイッチの PROFINET 機能をイネーブルにします。               |

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show profinet</b>  | スイッチの PROFINET セッションの詳細を表示します。  |

# debug profinet topology

PROFINET トポロジ ディスカバリで使用されるリンク層検出プロトコル (LLDP) および簡易ネットワーク管理プロトコル (SNMP) パケットに関する情報を表示するには、特権 EXEC モードで **debug profinet topology** コマンドを使用します。PROFINET 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 profinet topology**

**no debug profinet topology**

## 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

PROFINET デバッグは設定されていません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**undebug profinet topology** コマンドは、**no debug profinet topology** コマンドと同じです。

シスコのテクニカル サポート エンジニアの指示を受けた場合にのみ、このコマンドを使用してください。

このコマンドを使用する場合、シリアル ポート経由ではなく、イーサネット ポート経由で Telnet を使用して Cisco IOS ソフトウェアのコマンドライン インターフェイス (CLI) にアクセスします。

## 例

次の例では、PROFINET トポロジ ディスカバリのデバッグをイネーブルにする方法を示します。

```
Switch# debug profinet topology
```

## 関連コマンド

| コマンド                           | 説明   |
|--------------------------------|--|
| <b>debug profinet alarm</b>    | PROFINET アラームのデバッグをイネーブルにします。                    |
| <b>debug profinet cyclic</b>   | PROFINET 巡回パケットの送受信に関連するファンクション コールを表示します。       |
| <b>debug profinet error</b>    | PROFINET セッション エラーのデバッグをイネーブルにします。               |
| <b>debug profinet packet</b>   | PROFINET パケットのデバッグをイネーブルにします。                    |
| <b>debug profinet platform</b> | Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにします。 |
| <b>debug profinet trace</b>    | トレースした一連のデバッグ出力ログを表示します。                         |
| <b>profinet</b>                | スイッチの PROFINET 機能をイネーブルにします。                     |

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show profinet</b>  | スイッチの PROFINET セッションの詳細を表示します。  |

# debug profinet trace

トレースされたデバッグ出力ログを表示するには、特権 EXEC モードで **debug profinet trace** コマンドを使用します。PROFINET 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 profinet trace**

**no debug profinet trace**

## 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

PROFINET デバッグは設定されていません。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**undebug profinet trace** コマンドは、**no debug profinet trace** コマンドと同じです。

シスコのテクニカル サポート エンジニアの指示を受けた場合にのみ、このコマンドを使用してください。

このコマンドを使用する場合、シリアル ポート経由ではなく、イーサネット ポート経由で Telnet を使用して Cisco IOS ソフトウェアのコマンドラインインターフェイス (CLI) にアクセスします。

## 例

次の例では、トレースされたデバッグ出力ログを表示する方法を示します。

```
Switch# debug profinet trace
```

## 関連コマンド

| コマンド                           | 説明   |
|--------------------------------|--|
| <b>debug profinet alarm</b>    | PROFINET アラームのデバッグをイネーブルにします。                    |
| <b>debug profinet cyclic</b>   | PROFINET 巡回パケットの送受信に関連するファンクション コールを表示します。       |
| <b>debug profinet error</b>    | PROFINET セッション エラーのデバッグをイネーブルにします。               |
| <b>debug profinet packet</b>   | PROFINET パケットのデバッグをイネーブルにします。                    |
| <b>debug profinet platform</b> | Cisco IOS ソフトウェアと PROFINET の相互作用のデバッグをイネーブルにします。 |
| <b>debug profinet topology</b> | 受信した PROFINET トポロジ パケットを表示します。                   |
| <b>profinet</b>                | スイッチの PROFINET 機能をイネーブルにします。                     |

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show profinet</b>  | スイッチの PROFINET セッションの詳細を表示します。  |

# debug ptp

高精度時間プロトコル (PTP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug ptp** 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 ptp {bmc | clock-correction | errors | event | messages | error | transparent-clock}**

**no debug ptp {bmc | clock-correction | errors | event | messages | error | transparent-clock}**

## 構文の説明

|                          |  |
|--------------------------|--|
| <b>bmc</b>               | PTP ベスト マスター クロック アルゴリズムのデバッグ メッセージを表示します。 |
| <b>clock-correction</b>  | PTP クロック 修正デバッグ メッセージを表示します。               |
| <b>collision</b>         | PTP ソースのコリジョンのメッセージを表示します。                 |
| <b>error</b>             | PTP エラー デバッグ メッセージを表示します。                  |
| <b>event</b>             | PTP ステート イベント デバッグ メッセージを表示します。            |
| <b>messages</b>          | PTP デバッグ メッセージを表示します。                      |
| <b>transparent-clock</b> | PTP トランスペアレント クロックのデバッグ メッセージを表示します。       |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが導入されました。 |

## 使用上のガイドライン

**undebug ptp** コマンドは、**no debug ptp** コマンドと同じです。

## 関連コマンド

| コマンド                                       | 説明                         |
|--|----------------------------|
| <a href="#">ptp (インターフェイス コンフィギュレーション)</a> | PTP クロック プロパティを設定します。      |
| <a href="#">show ptp</a>                   | ポートの PTP クロック プロパティを設定します。 |
| <a href="#">show ptp</a>                   | ポートに設定された PTP プロパティを表示します。 |

# 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、特権 EXEC モードで **debug qos-manager** 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}
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|                |                                      |
|----------------|--------------------------------------|
| <b>all</b>     | すべての QoS-manager デバッグ メッセージを表示します。   |
| <b>event</b>   | QoS-manager 関連イベント デバッグ メッセージを表示します。 |
| <b>verbose</b> | QoS マネージャ詳細デバッグ メッセージを表示します。         |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 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   |
|-----------------------|--|
| <b>show debugging</b> | 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。構文情報については、『Cisco IOS Software Command Reference, Release 15.0』を参照してください。 |

# debug spanning-tree

スパニングツリー アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug spanning-tree** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events |
exceptions | general | mstp | pvst+ | root | snmp | switch | synchronization | uplinkfast}
```

```
no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events |
exceptions | general | mstp | pvst+ | root | snmp | switch | synchronization | uplinkfast}
```

## 構文の説明

|                        |   |
|------------------------|---|
| <b>all</b>             | すべてのスパニングツリー デバッグ メッセージを表示します。  |
| <b>backbonefast</b>    | BackboneFast-event デバッグ メッセージを表示します。  |
| <b>bpdu</b>            | スパニングツリーブリッジプロトコル データ ユニット (BPDU) デバッグ メッセージを表示します。   |
| <b>bpdu-opt</b>        | 最適化された BPDU 処理デバッグ メッセージを表示します。   |
| <b>config</b>          | 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。   |
| <b>etherchannel</b>    | EtherChannel-support デバッグ メッセージを表示します。  |
| <b>events</b>          | 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。  |
| <b>exceptions</b>      | 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。   |
| <b>general</b>         | 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。  |
| <b>mstp</b>            | Multiple Spanning-Tree Protocol (MSTP) イベントをデバッグします。  |
| <b>pvst+</b>           | 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。  |
| <b>root</b>            | 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。   |
| <b>snmp</b>            | スパニングツリー簡易ネットワーク管理プロトコル (SNMP) 処理デバッグ メッセージを表示します。  |
| <b>synchronization</b> | 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。  |
| <b>switch</b>          | スイッチ シム コマンドのデバッグ メッセージを表示します。このシムは、一般的なスパニングツリー プロトコル (STP) コードと、各スイッチ プラットフォーム固有コードとの間のインターフェイスとなるソフトウェア モジュールです。 |
| <b>uplinkfast</b>      | UplinkFast-event デバッグ メッセージを表示します。  |



(注)

**csuf/csrt** 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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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  |
|--------|---------------------------------|---|
|        | <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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
|        | <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 backbonefast

スパニングツリー BackboneFast イベントのデバッグをイネーブルにするには、特権 EXEC モードで **debug spanning-tree backbonefast** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug spanning-tree backbonefast** [detail | exceptions]

**no debug spanning-tree backbonefast** [detail | exceptions]

## 構文の説明

|                   |  |
|-------------------|--|
| <b>detail</b>     | (任意) 詳細な BackboneFast デバッグ メッセージを表示します。        |
| <b>exceptions</b> | (任意) スパニングツリー BackboneFast 例外デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug spanning-tree backbonefast** コマンドは、**no debug spanning-tree backbonefast** コマンドと同じです。

## 関連コマンド

| コマンド                      | 説明  |
|---------------------------|---|
| <b>show debugging</b>     | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show spanning-tree</b> | スパニングツリー ステータス情報を表示します。   |

# debug spanning-tree bpdu

送受信されたスパンニングツリー ブリッジ プロトコル データ ユニット (BPDU) のデバッグをイネーブルにするには、特権 EXEC モードで **debug spanning-tree bpdu** 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

|                 |   |
|-----------------|---|
| <b>receive</b>  | (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。          |
| <b>transmit</b> | (任意) 送信された BPDU デバッグ メッセージについて、最適化されないパスを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|---------------------------|---|
| <b>show debugging</b>     | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show spanning-tree</b> | スパンニングツリー 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ブリッジプロトコルデータユニット (BPDU) 処理のデバッグをイネーブルにするには、特権 EXEC モードで **debug spanning-tree bpdu-opt** 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

|               |   |
|---------------|---|
| <b>detail</b> | (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。       |
| <b>packet</b> | (任意) パケット レベルの最適化された BPDU 処理デバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug spanning-tree bpdu-opt** コマンドは、**no debug spanning-tree bpdu-opt** コマンドと同じです。

## 関連コマンド

| コマンド                      | 説明  |
|---------------------------|---|
| <b>show debugging</b>     | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show spanning-tree</b> | スパニングツリー ステート情報を表示します。  |

# debug spanning-tree mstp

マルチ スパニングツリー プロトコル (MSTP) ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug spanning-tree mstp** 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

|                     |   |
|---------------------|---|
| <b>all</b>          | すべてのデバッグ メッセージをイネーブルにします。   |
| <b>boundary</b>     | 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"> <li>Multiple Spanning-Tree (MST) リージョンと、高速スパニングツリー プロトコル (RSTP) が稼働する単一のスパニングツリー リージョンとの境界</li> <li>MST リージョンと、802.1D が稼働する単一のスパニングツリー リージョンとの境界</li> <li>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</li> </ul> |
| <b>bpdu-rx</b>      | 受信した MST ブリッジ プロトコル データ ユニット (BPDU) をデバッグします。   |
| <b>bpdu-tx</b>      | 送信された MST BPDU をデバッグします。  |
| <b>errors</b>       | MSTP エラーをデバッグします。   |
| <b>flush</b>        | ポート フラッシュ メカニズムをデバッグします。  |
| <b>init</b>         | MSTP データ構造の初期化をデバッグします。   |
| <b>migration</b>    | プロトコル移行ステート マシンをデバッグします。  |
| <b>pm</b>           | MSTP ポート マネージャ イベントをデバッグします。  |
| <b>proposals</b>    | 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。   |
| <b>region</b>       | スイッチ プロセッサ (SP) とルート プロセッサ (RP) 間のリージョン同期をデバッグします。  |
| <b>roles</b>        | MSTP のロールをデバッグします。  |
| <b>sanity_check</b> | 受信した BPDU の健全性確認メッセージをデバッグします。  |
| <b>sync</b>         | ポート同期イベントをデバッグします。  |
| <b>tc</b>           | トポロジ変更通知イベントをデバッグします。   |
| <b>timers</b>       | 開始、停止、および期限切れイベントの MSTP タイマーをデバッグします。   |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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。

## ■ debug spanning-tree mstp

| 関連コマンド | コマンド                      | 説明  |
|--------|---------------------------|---|
|        | <b>show debugging</b>     | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
|        | <b>show spanning-tree</b> | スパニングツリー ステート情報を表示します。  |

# debug spanning-tree switch

スパニング ツリー プロトコル (STP) ソフトウェア モジュールとポート マネージャ ソフトウェア モジュール間のソフトウェア インターフェイスのデバッグをイネーブルにするには、特権 EXEC モードで **debug spanning-tree switch** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors |
interrupt | process} | state | tx [decode] | uplinkfast}
```

```
no debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors |
interrupt | process} | state | tx [decode] | uplinkfast}
```

## 構文の説明

|                    |   |
|--------------------|---|
| <b>all</b>         | すべてのスパニングツリー スイッチのデバッグ メッセージを表示します。   |
| <b>errors</b>      | 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。   |
| <b>flush</b>       | 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。   |
| <b>general</b>     | 一般イベント デバッグ メッセージを表示します。  |
| <b>helper</b>      | 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。  |
| <b>pm</b>          | 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。  |
| <b>rx</b>          | 受信したブリッジプロトコル データ ユニット (BPDU) 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"> <li>• <b>decode</b> : デコード済み受信パケットを表示します。</li> <li>• <b>errors</b> : 受信エラー デバッグ メッセージを表示します。</li> <li>• <b>interrupt</b> : 割り込みサービス要求 (ISR) デバッグ メッセージを表示します。</li> <li>• <b>process</b> : 処理受信 BPDU デバッグ メッセージを表示します。</li> </ul> |
| <b>state</b>       | 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。  |
| <b>tx [decode]</b> | 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"> <li>• <b>decode</b> : (任意) デコードされた送信パケットを表示します。</li> </ul>   |
| <b>uplinkfast</b>  | UplinkFast パケット送信デバッグ メッセージを表示します。  |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug spanning-tree switch** コマンドは、**no debug spanning-tree switch** コマンドと同じです。

## ■ debug spanning-tree switch

| 関連コマンド | コマンド                      | 説明  |
|--------|---------------------------|---|
|        | <b>show debugging</b>     | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
|        | <b>show spanning-tree</b> | スパニングツリー ステート情報を表示します。  |

# debug spanning-tree uplinkfast

スパニングツリー UplinkFast イベントのデバッグをイネーブルにするには、特権 EXEC モードで **debug spanning-tree uplinkfast** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**debug spanning-tree uplinkfast [exceptions]**

**no debug spanning-tree uplinkfast [exceptions]**

## 構文の説明

**exceptions** (任意) スパニングツリー UplinkFast 例外デバッグ メッセージを表示します。

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug spanning-tree uplinkfast** コマンドは、**no debug spanning-tree uplinkfast** コマンドと同じです。

## 関連コマンド

| コマンド                      | 説明  |
|---------------------------|---|
| <b>show debugging</b>     | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show spanning-tree</b> | スパニングツリー ステータス情報を表示します。   |

# debug sw-vlan

VLAN 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、特権 EXEC モードで **debug sw-vlan** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | mapping |
notification | packets | redundancy | registries | vtp}
```

```
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | mapping
| notification | packets | redundancy | registries | vtp}
```

## 構文の説明

|                                |  |
|--------------------------------|--|
| <b>badpmcookies</b>            | 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。   |
| <b>cfg-vlan {bootup   cli}</b> | 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"> <li><b>bootup</b> : 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。</li> <li><b>cli</b> : コマンドライン インターフェイス (CLI) が config-vlan モードである場合のメッセージを表示します。</li> </ul> |
| <b>events</b>                  | 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。  |
| <b>ifs</b>                     | <a href="#">debug sw-vlan ifs</a> コマンドを参照してください。   |
| <b>management</b>              | 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。   |
| <b>mapping</b>                 | VLAN マッピングのデバッグ メッセージを表示します。   |
| <b>notification</b>            | <a href="#">debug sw-vlan notification</a> コマンドを参照してください。  |
| <b>packets</b>                 | 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。   |
| <b>redundancy</b>              | VTP VLAN 冗長性のデバッグ メッセージを表示します。   |
| <b>registries</b>              | 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。   |
| <b>vtp</b>                     | <a href="#">debug sw-vlan vtp</a> コマンドを参照してください。   |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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。

## 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <code>show vlan</code>      | 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。   |
| <code>show vtp</code>       | VTP 管理ドメイン、ステータス、およびカウンタに関する一般情報を表示します。  |

# debug sw-vlan ifs

VLAN マネージャ Cisco 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、特権 EXEC モードで **debug sw-vlan ifs** 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

|                             |  |
|-----------------------------|--|
| <b>open {read   write}</b>  | 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"> <li><b>read</b> : 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。</li> <li><b>write</b> : 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。</li> </ul> |
| <b>read {1   2   3   4}</b> | 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。  |
| <b>write</b>                | ファイル書き込み動作のデバッグ メッセージを表示します。   |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug sw-vlan ifs** コマンドは、**no debug sw-vlan ifs** コマンドと同じです。

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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show vlan</b>      | 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

スイッチ間リンク (ISL) 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、特権 EXEC モードで **debug sw-vlan notification** 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 | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}**

**no debug sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}**

## 構文の説明

|                            |   |
|----------------------------|---|
| <b>accfwdchange</b>        | 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。 |
| <b>allowedvlanfgchange</b> | 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。                |
| <b>fwdchange</b>           | 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。                 |
| <b>linkchange</b>          | 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。              |
| <b>modechange</b>          | 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。                  |
| <b>pruningcfgchange</b>    | プルーニング設定変更の VLAN マネージャ通知のデバッグ メッセージを表示します。                      |
| <b>statechange</b>         | インターフェイス ステート変更の VLAN マネージャ通知のデバッグ メッセージを表示します。                 |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show vlan</b>      | 管理ドメインに設定されたすべての VLAN または特定の VLAN (VLAN 名または ID を指定した場合) のパラメータを表示します。  |

# debug sw-vlan vtp

VLAN トランッキング プロトコル (VTP) コードのデバッグをイネーブルにするには、EXEC モードで **debug sw-vlan vtp** 特権コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug sw-vlan vtp {events | packets | pruning [packets | xmit] | redundancy | xmit}
```

```
no debug sw-vlan vtp {events | packets | pruning | redundancy | xmit}
```

## 構文の説明

|                                 |  |
|---------------------------------|--|
| <b>events</b>                   | 汎用の論理フローのデバッグ メッセージおよび VTP コード内の VTP_LOG_RUNTIME マクロによって生成された VTP メッセージの詳細を表示します。  |
| <b>packets</b>                  | Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP パケット (プルーニング パケットを除く) の内容のデバッグ メッセージを表示します。   |
| <b>pruning [packets   xmit]</b> | VTP コードのプルーニング セグメントによって生成されるデバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>packets</b> : (任意) Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP プルーニング パケットの内容のデバッグ メッセージを表示します。</li> <li><b>xmit</b> : (任意) VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信 VTP パケットの内容のデバッグ メッセージを表示します。</li> </ul> |
| <b>redundancy</b>               | VTP 冗長性のデバッグ メッセージを表示します。  |
| <b>xmit</b>                     | VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信 VTP パケット (プルーニング パケットを除く) の内容のデバッグ メッセージを表示します。   |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug sw-vlan vtp** コマンドは、**no debug sw-vlan vtp** コマンドと同じです。

**pruning** キーワードの後にパラメータを指定しない場合は、VTP プルーニング デバッグ メッセージが表示されます。これらのメッセージは、VTP プルーニング コード内の VTP\_PRUNING\_LOG\_NOTICE、VTP\_PRUNING\_LOG\_INFO、VTP\_PRUNING\_LOG\_DEBUG、VTP\_PRUNING\_LOG\_ALERT、および VTP\_PRUNING\_LOG\_WARNING マクロによって生成されます。

## 関連コマンド

| コマンド                        | 説明   |
|-----------------------------|--|
| <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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <code>show vtp</code>       | VTP 管理ドメイン、ステータス、およびカウンタに関する一般情報を表示します。  |

# debug udld

単方向リンク検出 (UDLD) 機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug udld** 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

|                   |   |
|-------------------|---|
| <b>events</b>     | 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。   |
| <b>packets</b>    | 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。       |
| <b>registries</b> | UDLD プロセスが UDLD プロセスに依存するモジュールおよびその他のフィーチャ モジュールからのレジストリ コールを処理するときに、このプロセスのデバッグ メッセージを表示します。 |

## デフォルト

デバッグはディセーブルです。

## コマンドモード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

**undebug udld** コマンドは、**no debug udld** コマンドと同じです。

**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
- error-disable ステートの設定および消去のプログラム アクション
- ネイバー キャッシュの追加および削除
- コンフィギュレーション コマンドの処理
- リンクアップおよびリンクダウン通知処理

**debug udld packets** を入力すると、次に示すデバッグ メッセージが表示されます。

- 着信パケット受信時の一般的なパケット処理プログラム フロー
- 受信したパケットをパケット受信コードで調べるときの、各パケットの内容の識別情報 (Type Length Version (TLV) など)
- パケット送信の試行内容およびその成果

**debug udld registries** を入力すると、次に示すカテゴリのデバッグ メッセージが表示されます。

- サブブロックの作成

- ファイバポート ステータスの変更
- ポート マネージャ ソフトウェアからのステート変更通知情報
- MAC アドレス レジストリ コール

**関連コマンド**

| コマンド                  | 説明  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |
| <b>show uddld</b>     | 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、特権 EXEC モードで **debug vqpc** 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

|               |  |
|---------------|--|
| <b>all</b>    | (任意) VQP クライアント デバッグ メッセージを表示します。                        |
| <b>cli</b>    | (任意) VQP クライアント コマンドライン インターフェイス (CLI) デバッグ メッセージを表示します。 |
| <b>events</b> | (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。                   |
| <b>learn</b>  | (任意) VQP クライアント アドレス学習デバッグ メッセージを表示します。                  |
| <b>packet</b> | (任意) VQP クライアント パケット情報デバッグ メッセージを表示します。                  |

## デフォルト

デバッグはディセーブルです。

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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  |
|-----------------------|---|
| <b>show debugging</b> | 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。構文情報については、『 <i>Cisco IOS Software Command Reference, Release 15.0</i> 』を参照してください。 |



## APPENDIX **C**

# Cisco IE 2000 スイッチ show platform コマンド

---

この付録では、スイッチ用に作成または変更された **show platform** 特権 EXEC コマンドについて説明します。これらのコマンドは、インターネットワーキングの問題の診断および解決に役立つ情報を表示します。使用する場合には、必ずシスコのテクニカル サポート担当者の指示に従ってください。

# show platform acl

プラットフォームに依存するアクセス コントロール リスト (ACL) マネージャ情報を表示するには、特権 EXEC モードで **show platform acl** 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}
```

## 構文の説明

|  |   |
|--|---|
| <b>interface interface-id</b>              | 指定し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。  |
| <b>label label-number</b><br><b>detail</b> | ラベル単位の ACL マネージャ情報を表示します。label-number に指定できる範囲は 0 ~ 255 です。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>detail</b> : (任意) ACL マネージャ ラベル情報の詳細を表示します。</li> </ul> |
| <b>statistics asic-number</b>              | ASIC 単位の ACL マネージャ情報を表示します。asic-number に指定できる範囲は、0 または 1 のいずれかのポート ASIC 番号です。   |
| <b>usage asic-number</b><br><b>summary</b> | ASIC 単位の ACL 使用状況情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>summary</b> : (任意) 使用状況情報の概要を表示します。</li> </ul>  |
| <b>vlan vlan-id</b>                        | VLAN 単位の ACL マネージャ情報を表示します。vlan-id に指定できる範囲は 1 ~ 4094 です。   |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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 backup interface

Flex Link 設定で使用されてい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、特権 EXEC モードで **show platform backup interface** コマンドを使用します。

```
show platform backup interface [interface-id | dummyQ]
```

## 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したインターフェイスの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。 |
| <b>dummyQ</b>       | (任意) ダミー キュー情報を表示します。   |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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 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、特権 EXEC モードで **show platform configuration** コマンドを使用します。

**show platform configuration {config-output | default | running | startup}**

## 構文の説明

|                      |  |
|----------------------|--|
| <b>config-output</b> | 最後の自動設定アプリケーションの出力を表示します。                            |
| <b>default</b>       | 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。                       |
| <b>running</b>       | 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。        |
| <b>startup</b>       | 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。 |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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。



(注)

このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

# 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、特権 EXEC モードで **show platform etherchannel** コマンドを使用します。

```
show platform etherchannel {flags | time-stamps}
```

## 構文の説明

|                    |                              |
|--------------------|------------------------------|
| <b>flags</b>       | EtherChannel ポート フラグを表示します。  |
| <b>time-stamps</b> | EtherChannel タイム スタンプを表示します。 |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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 forward

指定したパラメータと一致したフレームをハードウェアで転送する方法を指定するには、インターフェイスに対して特権 EXEC モードで **show platform forward** コマンドを使用します。

```
show platform forward interface-id [vlan vlan-id] src-mac dst-mac [l3protocol-id] [ipv6 | sap |
snap] [cos cos] [ip src-ip dst-ip [frag field] [dscp dscp] {l4protocol-id | icmp icmp-type
icmp-code | igmp igmp-version igmp-type | sctp src-port dst-port | tcp src-port dst-port flags |
udp src-port dst-port}]
```

## 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)。   |
| <b>vlan</b> <i>vlan-id</i>                | (任意) 入力 VLAN ID を指定します。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。  |
| <b>ipv6</b>                               | (任意) IPv6 フレームを指定します。このキーワードは、スイッチで IP サービス イメージが稼働している場合にだけ使用できます。  |
| <b>sap</b>                                | (任意) サービス アクセス ポイント (SAP) カプセル化タイプを指定します。  |
| <b>snap</b>                               | (任意) サブネットワーク アクセス プロトコル (SNAP) カプセル化タイプを指定します。  |
| <b>cos</b> <i>cos</i>                     | (任意) フレームのサービス クラス (CoS) 値を指定します。指定できる範囲は 0 ~ 7 です。  |
| <b>ip</b> <i>src-ip 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 アドレスを指定します。  |
| <b>frag</b> <i>field</i>                  | (任意) フラグメント IP パケットの IP フラグメント フィールドを指定します。指定できる範囲は 0 ~ 65535 です。  |
| <b>dscp</b> <i>dscp</i>                   | (任意) IP ヘッダーの DiffServ コード ポイント (DSCP) フィールドを指定します。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 は総称ルーティング カプセル化 (GRE) であり、89 は Open Shortest Path First (OSPF) です。プロトコルが TCP、ユーザ データグラム プロトコル (UDP)、インターネット制御メッセージ プロトコル (ICMP)、またはインターネットグループ管理プロトコル (IGMP) である場合、数値の代わりに適切なキーワードを使用する必要があります。 |
| <b>icmp</b> <i>icmp-type icmp-code</i>    | ICMP パラメータを指定します。 <i>icmp-type</i> および <i>icmp-code</i> に指定できる範囲は 0 ~ 255 です。  |
| <b>igmp</b> <i>igmp-version igmp-type</i> | IGMP パラメータを指定します。指定できる範囲は、 <i>igmp-version</i> は 1 ~ 15、 <i>igmp-type</i> は 0 ~ 15 です。   |
| <b>sctp</b> <i>src-port dst-port</i>      | Stream Control Transmission Protocol(SCTP) パラメータを指定します。SCTP 送信元および宛先ポートに指定できる範囲は 0 ~ 65535 です。   |

|   |   |
|---|---|
| <b>tcp</b> <i>src-port dst-port flags</i> | TCP パラメータ (ヘッダーの TCP 送信元ポート、宛先ポート、TCP フラグ バイトの数値) を指定します。 <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。 |
| <b>udp</b> <i>src-port dst-port</i>       | UDP パラメータを指定します。 <i>src-port</i> および <i>dst-port</i> に指定できる範囲は 0 ~ 65535 です。  |

**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            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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。

**例** **show platform forward** コマンドの出力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 ip igmp snooping

プラットフォームに依存するインターネットグループ管理プロトコル (IGMP) スヌーピング情報を表示するには、特権 EXEC モードで **show platform ip igmp snooping** 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]]}
```

## 構文の説明

|                                  |   |
|----------------------------------|---|
| <b>all</b>                       | 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。   |
| <b>control di</b>                | 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"> <li><b>di</b> : (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。</li> </ul>                     |
| <b>counters</b>                  | IGMP スヌーピング カウンタを表示します。   |
| <b>flood vlan vlan-id</b>        | 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"> <li><b>vlan vlan-id</b> : (任意) 指定した 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。</li> </ul>   |
| <b>group ip-address</b>          | 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。   |
| <b>hardware</b>                  | 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。  |
| <b>retry count   local count</b> | 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"> <li><b>count</b> : (任意) 再試行回数だけを表示します。</li> <li><b>local</b> : (任意) ローカル再試行エントリを表示します。</li> </ul> |
| <b>remote count</b>              | 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"> <li><b>count</b> : (任意) リモート カウントだけを表示します。</li> </ul>  |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

# show platform ip unicast

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、特権 EXEC モードで **show platform ip unicast** コマンドを使用します。

```
show platform ip unicast {adjacency | cef-idb | counts | dhcp | failed {adjacency | arp [A.B.C.D]
| route} | loadbalance | mpaths | proxy | route | standby | statistics | table | trace}
```

| 構文の説明   |  |
|---|--|
| <b>adjacency</b>                              | プラットフォーム隣接データベースを表示します。  |
| <b>cef-idb</b>                                | シスコ エクスプレス フォワーディング (CEF) 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。  |
| <b>counts</b>                                 | レイヤ 3 ユニキャスト データベースの現在のカウンタを表示します。   |
| <b>dhcp</b>                                   | DHCP システム ダイナミック アドレスを表示します。   |
| <b>failed adjacency   arp A.B.C.D   route</b> | 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"> <li><b>adjacency</b> : 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。</li> <li><b>arp</b> : 障害および再試行によるアドレス解決プロトコル (ARP) の削除を表示します。</li> <li><b>A.B.C.D</b> : (任意) 表示する ARP エントリのプレフィックス。</li> <li><b>route</b> : 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。</li> </ul> |
| <b>loadbalance</b>                            | 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。  |
| <b>mpaths</b>                                 | 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。   |
| <b>proxy</b>                                  | プラットフォーム プロキシ ARP データベースを表示します。  |
| <b>route</b>                                  | プラットフォーム ルート データベースを表示します。   |
| <b>standby</b>                                | プラットフォーム スタンバイ情報を表示します。  |
| <b>statistics</b>                             | 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。   |
| <b>table</b>                                  | プラットフォーム IP version 4 (IPv4) 情報を表示します。   |
| <b>trace</b>                                  | プラットフォーム イベント トレース ログを表示します。   |

**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            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | このコマンドが追加されました。 |

**使用上のガイドライン** このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

## ■ show platform ip unicast

**(注)**

このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

# show platform ip unicast vrf compaction

圧縮要求キューおよび圧縮ステータスを表示するには、特権 EXEC モードで **show platform ip unicast vrf compaction** コマンドを使用します。

## show platform ip unicast vrf compaction

### 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

なし

### コマンド モード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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。



(注)

このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

# show platform ip unicast vrf tcam-label

PBR および VRF-Lite ラベルと、PBR で使用されているラベルの数を表示するには、特権 EXEC モードで **show platform ip unicast vrf tcam-label** コマンドを使用します。

## show platform ip unicast vrf tcam-label

### 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

なし

### コマンドモード

特権 EXEC

### コマンド履歴

| リリース      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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。



(注)

このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

# show platform ip wccp

プラットフォームに依存する Web Cache Communication Protocol (WCCP) の情報を表示するには、特権 EXEC モードで **show platform ip wccp** コマンドを使用します。

```
show platform ip wccp {detail | label}
```

## 構文の説明

|               |                           |
|---------------|---------------------------|
| <b>detail</b> | プラットフォーム WCCP の詳細を表示します。  |
| <b>label</b>  | プラットフォーム WCCP のラベルを表示します。 |

## 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      | 変更内容            |
|-----------|-----------------|
| 15.0(1)EY | 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。



(注) このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

# 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、特権 EXEC モードで **show platform ipv6 unicast** コマンドを使用します。このコマンドは、スイッチが IP サービスイメージを稼働している場合にのみ使用することができます。

```
show platform ipv6 unicast {adjacency [ipv6-prefix] | backwalk {adjacency | loadbalance} |
compress ipv6-prefix/prefix length | interface | loadbalance | mpath | retry {adjacency |
route} | route [ipv6-prefix/prefix length | tcam] [detail] | statistics | table [detail] | trace}
```

## 構文の説明

|   |   |
|---|---|
| <b>adjacency</b>                                    | スイッチまたは指定した 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) IPv6 ネットワークを表示します。この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。  |
| <b>backwalk adjacency   loadbalance</b>             | IPv6 バックウォーク情報を表示します。 <ul style="list-style-type: none"> <li><b>adjacency</b> : 隣接バックウォーク情報を表示します。</li> <li><b>loadbalance</b> : バックウォーク ロードバランス情報を表示します。</li> </ul>  |
| <b>compress</b><br><i>ipv6-prefix/prefix length</i> | IPv6 プレフィックス圧縮情報を表示します。 <ul style="list-style-type: none"> <li><i>ipv6-prefix</i> : IPv6 ネットワークです。</li> <li><i>/prefix length</i> : IPv6 ネットワーク プレフィックスの長さです。アドレスの上位何ビットがプレフィックス (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。</li> </ul> |
| <b>interface</b>                                    | IPv6 インターフェイスの情報を表示します。   |
| <b>loadbalance</b>                                  | IPv6 のロード バランシングに関する情報を表示します。   |
| <b>mpath</b>  | IPv6 マルチパス情報を表示します。   |
| <b>retry adjacency   route</b>                      | IPv6 リトライ情報を表示します。 <ul style="list-style-type: none"> <li><b>adjacency</b> : IPv6 隣接リトライ情報を表示します。</li> <li><b>route</b> : IPv6 ルート リトライ情報を表示します。</li> </ul>   |
| <b>route</b>  | IPv6 ルート情報を表示します。   |
| <b>tcam</b>   | (任意) IPv6 TCAM ルート テーブル情報を表示します。  |
| <b>detail</b>                                       | (任意) IPv6 ルート情報の詳細を表示します。   |
| <b>statistics</b>                                   | IPv6 累積統計を表示します。  |
| <b>table</b>  | IPv6 ユニキャスト テーブル情報を表示します。   |
| <b>trace</b>  | IPv6 ユニキャスト トレースを表示します。   |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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。

**(注)**

このコマンドは、スイッチが IP サービス イメージを実行している場合だけ使用可能です。

# 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、特権 EXEC モードで **show platform layer4op** コマンドを使用します。

```
show platform layer4op {acl | pacl [port-asic] | qos [port-asic]} {and-or | map | or-and | vcu}
```

## 構文の説明

|                       |   |
|-----------------------|---|
| <b>acl</b>            | アクセス コントロール リスト (ACL) レイヤ 4 演算子情報を表示します。  |
| <b>pacl port-asic</b> | ポート ACL レイヤ 4 演算子情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><i>port-asic</i> : (任意) ポート ASIC 番号を表示します。</li> </ul>                      |
| <b>qos port-asic</b>  | 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"> <li><i>port-asic</i> : (任意) QoS ポート ASIC 番号を表示します。</li> </ul> |
| <b>and-or</b>         | AND-OR レジスタ情報を表示します。  |
| <b>map</b>            | 選択マップ情報を表示します。  |
| <b>or-and</b>         | OR-AND レジスタ情報を表示します。  |
| <b>vcu</b>            | Value Compare Unit (VCU) レジスタ情報を表示します。  |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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 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、特権 EXEC モードで **show platform mac-address-table** 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]
```

## 構文の説明

|                                       |   |
|---------------------------------------|---|
| <b>aging-array</b>                    | (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。   |
| <b>hash-table</b>                     | (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。   |
| <b>mac-address <i>mac-address</i></b> | (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。 |
| <b>vlan <i>vlan-id</i></b>            | (任意) 指定した VLAN の情報を表示します。指定できる範囲は 1 ~ 4094 です。                                      |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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 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、特権 EXEC モードで **show platform messaging** コマンドを使用します。

```
show platform messaging {application [incoming | outgoing | summary] | hipperf [class-number]}
```

## 構文の説明

|  |  |
|--|--|
| <b>application incoming   outgoing   summary</b> | 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"> <li><b>incoming</b> : (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。</li> <li><b>outgoing</b> : (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。</li> <li><b>summary</b> : (任意) すべてのアプリケーション メッセージング要求に関するサマリー情報を表示します。</li> </ul> |
| <b>hipperf [class-number]</b>                    | 発信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。  |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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 monitor

プラットフォームに依存するスイッチド ポート アナライザ (SPAN) 情報を表示するには、特権 EXEC モードで **show platform monitor** コマンドを使用します。

**show platform monitor** [*session session-number*]

|       |   |   |
|-------|---|---|
| 構文の説明 | <b>session</b><br><i>session-number</i> | (任意) 指定した 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。 |
|-------|---|---|

|       |    |
|-------|----|
| 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            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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 mvr table

プラットフォームに依存するマルチキャスト VLAN レジストレーション (MVR) マルチエクspansion 記述子 (MED) グループ マッピング テーブルを表示するには、特権 EXEC モードで **show platform mvr table** コマンドを使用します。

## show platform mvr table

### 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

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            |
|-----------|-----------------|
| 15.0(1)EY | 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 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、特権 EXEC モードで **show platform pm** 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}}
```

## 構文の説明

|  |   |
|--|---|
| <b>counters</b>                        | モジュール カウンタ情報を表示します。   |
| <b>group-masks</b>                     | EtherChannel グループ マスク情報を表示します。  |
| <b>idbs active-idbs   deleted-idbs</b> | 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"> <li><b>active-idbs</b> : アクティブ IDB 情報を表示します。</li> <li><b>deleted-idbs</b> : 削除または漏えいされた IDB 情報を表示します。</li> </ul> |
| <b>if-numbers</b>                      | インターフェイス番号情報を表示します。   |
| <b>link-status</b>                     | ローカル ポートのリンク ステータス情報を表示します。   |
| <b>platform-block</b>                  | プラットフォーム ポート ブロック情報を表示します。  |
| <b>port-info interface-id</b>          | 指定し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。  |
| <b>vlan info   line-state</b>          | 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"> <li><b>info</b> : アクティブ VLAN の情報を表示します。</li> <li><b>line-state</b> : ラインステート情報を表示します。</li> </ul>                              |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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。



(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。

# show platform port-asic

プラットフォームに依存するポート ASIC レジスタ情報を表示するには、特権 EXEC モードで **show platform port-asic** 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]]
  version}
```

## 構文の説明

|  |   |
|--|---|
| <b>cpu-queue-map-table</b><br>[asic number   port number<br>[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"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。</li> </ul>                               |
| <b>dest-map index number</b>   | 指定し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。   |
| <b>etherchannel-info</b> [asic number  <br>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"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul> |
| <b>exception</b> [asic number   port<br>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"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul>        |

|   |   |
|---|---|
| <b>global-status</b> [ <i>asic number</i>   <b>port number</b> [ <i>asic number</i> ]]    | <p>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。</p> <ul style="list-style-type: none"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul>   |
| <b>learning</b> [ <i>asic number</i>   <b>port number</b> [ <i>asic number</i> ]]         | <p>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。</p> <ul style="list-style-type: none"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul>     |
| <b>mac-info</b> [ <i>asic number</i>   <b>port number</b> [ <i>asic number</i> ]]         | <p>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。</p> <ul style="list-style-type: none"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul>     |
| <b>mvid</b> [ <i>asic number</i> ]  | <p>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。</p> <ul style="list-style-type: none"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> </ul>   |
| <b>packet-info-ram</b> [ <i>asic number</i>   <b>index number</b> [ <i>asic number</i> ]] | <p>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。</p> <ul style="list-style-type: none"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>index number</b> : (任意) 指定したパケット 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。</li> </ul>                     |
| <b>port-info</b> [ <i>asic number</i>   <b>port number</b> [ <i>asic number</i> ]]        | <p>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。</p> <ul style="list-style-type: none"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul>        |
| <b>prog-parser</b> [ <i>asic number</i>   <b>port number</b> [ <i>asic number</i> ]]      | <p>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。</p> <ul style="list-style-type: none"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul> |

|  |  |
|--|--|
| <b>receive</b> { <b>buffer-queue</b>   <b>port-fifo</b>   <b>supervisor-sram</b> } [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]]       | <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"> <li>• <b>buffer-queue</b> : バッファ キュー情報を表示します。</li> <li>• <b>port-fifo</b> : ポート FIFO 情報を表示します。</li> <li>• <b>supervisor-sram</b> : スーパーバイザ Static RAM (SRAM) 情報を表示します。</li> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul>                         |
| <b>span</b> [ <b>vlan-id</b>   <b>asic number</b> ]  | <p>スイッチド ポート アナライザ (SPAN) 関連情報を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>vlan-id</b> : (任意) 指定した VLAN の情報を表示します。指定できる範囲は 0 ~ 1023 です。</li> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> </ul>   |
| <b>stats</b> { <b>drop</b>   <b>enqueue</b>   <b>miscellaneous</b>   <b>supervisor</b> } [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]] | <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"> <li>• <b>drop</b> : ドロップ統計情報を表示します。</li> <li>• <b>enqueue</b> : エンキュー統計情報を表示します。</li> <li>• <b>miscellaneous</b> : 各種統計情報を表示します。</li> <li>• <b>supervisor</b> : スーパーバイザ統計情報を表示します。</li> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul> |
| <b>transmit</b> { <b>port-fifo</b>   <b>queue</b>   <b>supervisor-sram</b> } [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]]             | <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"> <li>• <b>port-fifo</b> : ポート FIFO 情報レジスタの内容を表示します。</li> <li>• <b>queue</b> : キュー情報レジスタの内容を表示します。</li> <li>• <b>supervisor-sram</b> : スーパーバイザ SRAM 情報を表示します。</li> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul>                                    |

|  |  |
|--|--|
| <b>vct</b> [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]] | 指定した ASIC または指定したポートおよび 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"> <li>• <b>asic number</b> : (任意) 指定した ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port number</b> : (任意) 指定したポートおよび 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。</li> </ul> |
| <b>version</b>   | ポート ASIC のバージョンおよびデバイス タイプ情報を表示します。  |

**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            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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。



(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。

# 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、特権 EXEC モードで **show platform port-security** コマンドを使用します。

## show platform 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

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            |
|-----------|-----------------|
| 15.0(1)EY | 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 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、特権 EXEC モードで **show platform qos** コマンドを使用します。

```
show platform qos {label asic number | policer {parameters asic number |
port alloc number asic number}}
```



(注)

このコマンドを使用できるのは、スイッチが LAN Base イメージを実行している場合だけです。

## 構文の説明

|   |   |
|---|---|
| <b>label asic number</b>  | 指定した ASIC の QoS ラベル マップを表示します。<br>(任意) <b>asic number</b> に指定できる範囲は 0 ~ 1 です。   |
| <b>policer {parameters asic number   port alloc number asic number}</b> | 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"> <li>• <b>parameters asic number</b> : 指定した ASIC のパラメータ情報を表示します。指定できる範囲は 0 ~ 1 です。</li> <li>• <b>port alloc number asic number</b> : 指定したポートおよび ASIC のポート割り当て情報を表示します。ポート割り当てに指定できる範囲は 0 ~ 25 です。ASIC に指定できる範囲は 0 ~ 1 です。</li> </ul> |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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 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、特権 EXEC モードで **show platform resource-manager** 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]}
```

## 構文の説明

|   |   |
|---|---|
| <b>dm</b> [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"> <li><b>index number</b> : (任意) 指定し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。</li> </ul>  |
| <b>erd</b> [index number]   | 指定したインデックスの等コスト 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"> <li><b>index number</b> : (任意) 指定し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。</li> </ul>   |
| <b>mad</b> [index number]   | 指定したインデックスの 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"> <li><b>index number</b> : (任意) 指定し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。</li> </ul>  |
| <b>med</b> [index number]   | 指定したインデックスのマルチエクステンション記述子テーブルを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>index number</b> : (任意) 指定し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。</li> </ul>  |
| <b>mod</b>  | リソース マネージャ モジュール情報を表示します。   |
| <b>msm</b> {hash-table [vlan vlan-id]   mac-address mac-address [vlan vlan-id]} | MAC アドレス記述子テーブルおよびステーション記述子テーブル情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>hash-table [vlan vlan-id]</b> : すべての VLAN または指定した VLAN のハッシュ テーブルを表示します。指定できる範囲は 1 ~ 4094 です。</li> <li><b>mac-address mac-address [vlan vlan-id]</b> : すべての VLAN または指定した VLAN に対する、48 ビット ハードウェア アドレスで表される指定した MAC アドレスの MAC アドレス記述子テーブルを表示します。指定できる範囲は 1 ~ 4094 です。</li> </ul> |
| <b>sd</b> [index number]  | 指定し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"> <li><b>index number</b> : (任意) 指定し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。</li> </ul>   |
| <b>vld</b> [index number]   | 指定したインデックスの 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"> <li><b>index number</b> : (任意) 指定し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。</li> </ul>  |

## デフォルト

なし

---

**コマンドモード**      特権 EXEC

---

| <b>コマンド履歴</b> | <b>リリース</b> | <b>変更箇所</b>     |
|---------------|-------------|-----------------|
|               | 15.0(1)EY   | 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 sdflesh

プラットフォーム SD フラッシュ情報を表示するには、特権 EXEC モードで **show platform sdflesh** コマンドを使用します。

**show platform sdflesh {status}**

|              |               |                    |
|--------------|---------------|--------------------|
| <b>構文の説明</b> | <b>status</b> | SD フラッシュの状態を表示します。 |
|--------------|---------------|--------------------|

|              |    |
|--------------|----|
| <b>デフォルト</b> | なし |
|--------------|----|

|                |         |
|----------------|---------|
| <b>コマンドモード</b> | 特権 EXEC |
|----------------|---------|

| <b>コマンド履歴</b> | リリース      | 変更内容            |
|---------------|-----------|-----------------|
|               | 15.0(1)EY | このコマンドが導入されました。 |

|                   |   |
|-------------------|---|
| <b>使用上のガイドライン</b> | 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。 |
|-------------------|---|

|          |                                    |
|----------|------------------------------------|
| <b>例</b> | 次に、プラットフォーム SD フラッシュ情報を表示する例を示します。 |
|----------|------------------------------------|

```
Switch# show platform sdflesh
SD Flash not present
Switch#
```

# show platform snmp counters

プラットフォームに依存する簡易ネットワーク管理プロトコル (SNMP) カウンタ情報を表示するには、特権 EXEC モードで **show platform snmp counters** コマンドを使用します。

## show platform snmp counters

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

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            |
|-----------|-----------------|
| 15.0(1)EY | 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 spanning-tree

プラットフォームに依存するスパニングツリー情報を表示するには、特権 EXEC モードで **show platform spanning-tree** コマンドを使用します。

**show platform spanning-tree synchronization [detail | vlan *vlan-id*]**

|              |  |   |
|--------------|--|---|
| <b>構文の説明</b> | <b>synchronization</b><br><b>[detail   vlan</b><br><i>vlan-id</i> <b>]</b> | スパニングツリー ステート同期情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>detail</b> : (任意) スパニングツリー情報の詳細を表示します。</li> <li>• <b>vlan <i>vlan-id</i></b> : (任意) 指定した VLAN の VLAN スイッチ スパニングツリー情報を表示します。指定できる範囲は 1 ~ 4094 です。</li> </ul> |
|--------------|--|---|

**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      | 変更内容            |
|--------|-----------|-----------------|
|        | 15.0(1)EY | 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 stp-instance

プラットフォームに依存するスパニングツリー インスタンス情報を表示するには、特権 EXEC モードで **show platform stp-instance** コマンドを使用します。

**show platform stp-instance *vlan-id***

|                   |   |  |
|-------------------|---|--|
| <b>構文の説明</b>      | <i>vlan-id</i>  | 指定した VLAN のスパニングツリー インスタンス情報を表示します。指定できる範囲は 1 ~ 4094 です。 |
| <b>デフォルト</b>      | なし  |  |
| <b>コマンド モード</b>   | 特権 EXEC   |  |
| <b>コマンド履歴</b>     | <b>リリース</b><br>15.0(1)EY  | <b>変更箇所</b><br>このコマンドが追加されました。                           |
| <b>使用上のガイドライン</b> | 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 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、特権 EXEC モードで **show platform tcam** コマンドを使用します。

```
show platform tcam {handle number | log-results | table {acl | all | equal-cost-route | ipv6 {qos |
secondary} 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]]
```

```
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]]
```

```
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]]
```

```
show platform tcam table ipv6 {qos | secondary} [asic number [detail [invalid]] | [index number
[detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]]
```

```
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]]
```

```
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]]
```

```
show platform tcam table multicast-expansion [asic number [detail [invalid]] | [index number
[detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]]
```

```
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]]
```

```
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]]
```

```
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]]
```

```
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]]
```

## 構文の説明

|                             |   |
|-----------------------------|---|
| <b>handle <i>number</i></b> | TCAM ハンドルを表示します。指定できる範囲は 0 ~ 4294967295 です。 |
| <b>log-results</b>          | TCAM ログ結果を表示します。                            |

**table** {acl | all | equal-cost-route | ipv6 {qos | secondary} local | mac-address | multicast-expansion | qos | secondary | station | vlan-list}

ルックアップおよび転送テーブル情報を表示します。キーワードの意味は次のとおりです。

- **all** : すべての TCAM テーブルを表示します。
- **equal-cost-route** : 等価コスト ルート テーブルを表示します。
- **ipv6** : IPv6 情報を表示します。
  - **qos** : IPv6 QoS テーブル情報を表示します。
  - **secondary** : IPv6 セカンダリ テーブル情報を表示します。
- **local** : ローカル テーブルを表示します。
- **mac-address** : MAC アドレス テーブルを表示します。
- **multicast-expansion** : IPv6 マルチキャスト拡張テーブルを表示します。
- **qos** : QoS テーブルを表示します。
- **secondary** : セカンダリ テーブルを表示します。
- **station** : ステーション テーブルを表示します。
- **vlan-list** : VLAN リストのテーブルを表示します。

#### usage

CAM (連想メモリ) および転送テーブル使用状況を表示します。

[[asic number [detail [invalid]] | index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid]] | [num number [detail [invalid]] | invalid]]

情報を表示します。キーワードの意味は次のとおりです。

- **asic number** : 指定した ASIC 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) 指定した 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) 指定した 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。

#### 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

15.0(1)EY

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。



(注)

**usage** 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。

# 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、特権 EXEC モードで **show platform vlan** コマンドを使用します。

```
show platform vlan {misc | mvid | prune | refcount | rpc {receive | transmit}}
```

## 構文の説明

|                                 |   |
|---------------------------------|---|
| <b>misc</b>                     | 各種 VLAN モジュール情報を表示します。  |
| <b>mvid</b>                     | マッピングされた VLAN ID (MVID) 割り当て情報を表示します。   |
| <b>prune</b>                    | プラットフォームで維持されるブルーニング データベースを表示します。  |
| <b>refcount</b>                 | 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。   |
| <b>rpc {receive   transmit}</b> | リモート プロシージャ コール (RPC) 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"> <li><b>receive</b> : 受信した情報を表示します。</li> <li><b>transmit</b> : 送信した情報を表示します。</li> </ul> |

## 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            |
|-----------|-----------------|
| 15.0(1)EY | 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。



## APPENDIX **D**

# オープン ソース ソフトウェアについて

---

Cisco IOS ソフトウェアの pipe コマンドは、Henry Spencer の正規表現ライブラリ (regex) を使用しています。このライブラリの最新版は、ライブラリの旧バージョンとの互換性を保つために Catalyst オペレーティング システム ソフトウェアで若干修正されています。

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.





## INDEX

### A

aaa accounting dot1x コマンド [2-1](#)  
aaa authentication dot1x コマンド [2-3](#)  
aaa authorization network コマンド [2-5, 2-34, 2-40, 2-42, 2-44, 2-46, 2-48, 2-138, 2-295, 2-491, B-8, B-36](#)  
AAA 方式 [2-3](#)  
ACE [2-129, 2-399](#)  
ACL  
    deny コマンド [2-127](#)  
    IP [2-188](#)  
    許可 [2-397](#)  
    照合 [2-326](#)  
    非 IP プロトコル対応 [2-299](#)  
    表示 [2-467](#)  
    レイヤ 2 インターフェイス上 [2-188](#)  
action コマンド [2-6](#)  
alarm contact コマンド [2-8](#)  
alarm facility fcs-hysteresis コマンド [2-10, 2-11](#)  
alarm facility input-alarm コマンド [2-11, 2-14](#)  
alarm facility power-supply コマンド [2-12](#)  
alarm facility temperature コマンド [2-15](#)  
alarm profile  
    作成 [2-17](#)  
    表示 [2-471](#)  
    ポートへの接続 [2-19](#)  
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 [2-19](#)  
alarm profile (グローバル コンフィギュレーション) コマンド [2-17](#)  
alarm profile コンフィギュレーション モード [2-17](#)  
alarm relay-mode  
    設定 [2-21](#)  
alarm relay-mode コマンド [2-21](#)

alarm コマンド [2-17](#)  
archive download-sw コマンド [2-22](#)  
archive tar コマンド [2-25](#)  
archive upload-sw コマンド [2-28](#)  
arp access-list コマンド [2-30](#)  
authentication command bounce-port ignore [2-32](#)  
authentication command disable-port ignore [2-33](#)  
authentication control-direction コマンド [2-34](#)  
authentication event コマンド [2-36](#)  
authentication fallback コマンド [2-40](#)  
authentication host-mode コマンド [2-42](#)  
authentication mac-move permit コマンド [2-44](#)  
authentication open コマンド [2-46](#)  
authentication order コマンド [2-48](#)  
authentication periodic コマンド [2-50](#)  
authentication port-control コマンド [2-52](#)  
authentication priority コマンド [2-54](#)  
authentication timer コマンド [2-56](#)  
authentication violation コマンド [2-58](#)  
auth-fail max-attempts コマンド  
    「dot1x auth-fail max-attempts コマンド」を参照  
auth-fail vlan  
    「dot1x auth-fail vlan」を参照  
auth open コマンド [2-46](#)  
auth order コマンド [2-48](#)  
auth timer コマンド [2-56](#)  
auto qos voip コマンド [2-60](#)

### B

BackboneFast、STP 用 [2-718](#)  
boot buffersize コマンド [2-65](#)  
boot config-file コマンド [2-66](#)

boot enable-break コマンド [2-67](#)  
 boot fast コマンド [2-68](#)  
 boot helper-config file コマンド [2-70](#)  
 boot helper コマンド [2-69](#)  
 boot manual コマンド [2-72](#)  
 boot private-config-file コマンド [2-73](#)  
 boot system コマンド [2-74](#)  
 boot (ブートローダ) コマンド [A-2](#)  
 BPDU ガード、スパニングツリー用 [2-721, 2-750](#)  
 BPDU フィルタリング、スパニングツリー用 [2-719, 2-750](#)

---

## C

cat (ブートローダ) コマンド [A-4](#)  
 channel-group コマンド [2-75](#)  
 channel-protocol コマンド [2-79](#)  
 Cisco SoftPhone  
     auto-QoS の設定 [2-60](#)  
     送信されたパケットを信頼する [2-366](#)  
 CISP  
     「Client Information Signalling Protocol」を参照  
     debug platform cisp コマンド [B-36](#)  
 cisp  
     enable コマンド [2-82](#)  
 class-map コマンド [2-85](#)  
 class コマンド [2-83](#)  
 clear dot1x コマンド [2-87](#)  
 clear eap sessions コマンド [2-88](#)  
 clear errdisable interface [2-89](#)  
 clear ip arp inspection log コマンド [2-90](#)  
 clear ip arp inspection statistics コマンド [2-91](#)  
 clear ipc コマンド [2-94](#)  
 clear ip dhcp snooping database コマンド [2-92](#)  
 clear ipv6 dhcp conflict コマンド [2-95](#)  
 clear lacp コマンド [2-96](#)  
 clear mac address-table コマンド [2-97, 2-98](#)  
 clear nmsp statistics コマンド [2-99](#)  
 clear pagp コマンド [2-100, 2-104](#)

clear port-security コマンド [2-101](#)  
 clear psp counter [2-103](#)  
 clear psp counter コマンド [2-103](#)  
 clear spanning-tree counters コマンド [2-105](#)  
 clear spanning-tree detected-protocols コマンド [2-106](#)  
 clear vmps statistics コマンド [2-108](#)  
 clear vtp counters コマンド [2-109](#)  
 Client Information Signalling Protocol [2-82, 2-138, 2-491, B-8, B-36](#)  
 cluster commander-address コマンド [2-110](#)  
 cluster discovery hop-count コマンド [2-112](#)  
 cluster enable コマンド [2-113](#)  
 cluster holdtime コマンド [2-114](#)  
 cluster member コマンド [2-115](#)  
 cluster outside-interface コマンド [2-117](#)  
 cluster run コマンド [2-118](#)  
 cluster standby-group コマンド [2-119](#)  
 cluster timer コマンド [2-121](#)  
 config-vlan モード  
     コマンド [2-820](#)  
 copy (ブートローダ) コマンド [A-6](#)  
 CoS  
     着信値の上書き [2-336](#)  
     着信パケットへのデフォルト値の割り当て [2-336](#)  
 CoS/DSCP マップ [2-340](#)  
 CPU ASIC 統計、表示 [2-499](#)  
 crashinfo ファイル [2-175](#)

---

## D

debug authentication [B-2](#)  
 debug auto qos コマンド [B-4](#)  
 debug backup コマンド [B-6, B-7](#)  
 debug cip [B-7](#)  
 debug cisp コマンド [B-8](#)  
 debug cluster コマンド [B-9](#)  
 debug dot1x コマンド [B-11](#)  
 debug dtp コマンド [B-12](#)  
 debug eap コマンド [B-13, B-86](#)

- debug etherchannel コマンド [B-14](#)
- debug interface コマンド [B-15](#)
- debug ip dhcp snooping コマンド [B-16](#)
- debug ip igmp filter コマンド [B-18](#)
- debug ip igmp max-groups コマンド [B-19](#)
- debug ip igmp snooping コマンド [B-20](#)
- debug ip verify source packet コマンド [B-17](#)
- debug l2nat コマンド [B-21](#)
- debug lacp コマンド [B-22](#)
- debug lldp packets コマンド [B-23](#)
- debug mac-notification コマンド [B-24](#)
- debug matm move update コマンド [B-26](#)
- debug matm コマンド [B-25](#)
- debug monitor コマンド [B-27](#)
- debug mvrdbg コマンド [B-29](#)
- debug nmsp コマンド [B-30](#)
- debug nvram コマンド [B-31](#)
- debug pagp コマンド [B-32](#)
- debug platform acl コマンド [B-33](#)
- debug platform backup interface コマンド [B-35](#)
- debug platform cisp コマンド [B-36](#)
- debug platform cpu-queues コマンド [B-37](#)
- debug platform dot1x コマンド [B-39](#)
- debug platform etherchannel コマンド [B-40](#)
- debug platform forw-tcam コマンド [B-41](#)
- debug platform ip arp inspection コマンド [B-42](#)
- debug platform ip dhcp コマンド [B-43](#)
- debug platform ip igmp snooping コマンド [B-44](#)
- debug platform ip source-guard コマンド [B-46](#)
- debug platform ip unicast コマンド [B-47](#)
- debug platform led コマンド [B-49](#)
- debug platform matm コマンド [B-50](#)
- debug platform messaging application コマンド [B-51](#)
- debug platform phy コマンド [B-52](#)
- debug platform pm コマンド [B-54](#)
- debug platform port-asic コマンド [B-56](#)
- debug platform port-security コマンド [B-57](#)
- debug platform qos-acl-tcam コマンド [B-58](#)
- debug platform resource-manager コマンド [B-59](#)
- debug platform snmp コマンド [B-60](#)
- debug platform span コマンド [B-61](#)
- debug platform supervisor-asic コマンド [B-62](#)
- debug platform sw-bridge コマンド [B-63](#)
- debug platform tcam コマンド [B-64](#)
- debug platform uddl コマンド [B-67](#)
- debug platform vlan コマンド [B-68](#)
- debug pm コマンド [B-69](#)
- debug port-security コマンド [B-71](#)
- debug profinet alarm [B-72](#)
- debug profinet cyclic [B-74](#)
- debug profinet error [B-76](#)
- debug profinet packet [B-78](#)
- debug profinet platform [B-80](#)
- debug profinet topology [B-82](#)
- debug profinet trace [B-84](#)
- debug qos-manager コマンド [B-87](#)
- debug spanning-tree backbonefast コマンド [B-90](#)
- debug spanning-tree bpdu-opt コマンド [B-92](#)
- debug spanning-tree bpdu コマンド [B-91](#)
- debug spanning-tree mstp コマンド [B-93](#)
- debug spanning-tree switch コマンド [B-95](#)
- debug spanning-tree uplinkfast コマンド [B-97](#)
- debug spanning-tree コマンド [B-88](#)
- debug sw-vlan ifs コマンド [B-100](#)
- debug sw-vlan notification コマンド [B-101](#)
- debug sw-vlan vtp コマンド [B-102](#)
- debug sw-vlan コマンド [B-98](#)
- debug udld コマンド [B-104](#)
- debug vqpc コマンド [B-106](#)
- defaultPort プロファイル [2-18, 2-19](#)
- define interface-range コマンド [2-122](#)
- delete コマンド [2-124](#)
- delete (ブートローダ) 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 [2-125](#)
- deny コマンド [2-127](#)
- DHCP スヌーピング  
イネーブル化

- VLAN 上 [2-222](#)
  - インターフェイス上で信頼 [2-220](#)
  - オプション 82 [2-214, 2-216](#)
  - エラー回復タイマー [2-172](#)
  - レート制限 [2-219](#)
  - 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 [2-92](#)
    - 更新 [2-436](#)
    - データベース エージェント、設定 [2-212](#)
    - バインディング
      - 削除 [2-210](#)
      - 追加 [2-210](#)
      - 表示 [2-555](#)
    - バインディング ファイル、設定 [2-212](#)
    - 表示
      - データベース エージェント ステータス [2-557, 2-559](#)
      - バインディング エントリ [2-555](#)
  - dir (ブートローダ) コマンド [A-8](#)
  - dot1x auth-fail max-attempts コマンド [2-132](#)
  - dot1x auth-fail vlan [2-134](#)
  - dot1x control-direction コマンド [2-136](#)
  - dot1x credentials (グローバル コンフィギュレーション) コマンド [2-138](#)
  - dot1x critical インターフェイス コンフィギュレーション コマンド [2-141](#)
  - dot1x critical グローバル コンフィギュレーション コマンド [2-139](#)
  - dot1x default コマンド [2-143](#)
  - dot1x fallback コマンド [2-144](#)
  - dot1x guest-vlan コマンド [2-145](#)
  - dot1x host-mode コマンド [2-147](#)
  - dot1x initialize コマンド [2-149](#)
  - dot1x mac-auth-bypass コマンド [2-150](#)
  - dot1x max-reauth-req コマンド [2-152](#)
  - dot1x max-req コマンド [2-153](#)
  - dot1x pae コマンド [2-154](#)
  - dot1x port-control コマンド [2-155](#)
  - dot1x re-authenticate コマンド [2-157](#)
  - dot1x reauthentication コマンド [2-158](#)
  - dot1x test eapol-capable コマンド [2-159](#)
  - dot1x test timeout コマンド [2-160](#)
  - dot1x timeout コマンド [2-161](#)
  - dot1x violation-mode コマンド [2-163](#)
  - dot1x コマンド [2-130](#)
  - DSCP/CoS マップ [2-340](#)
  - DSCP/DSCP 変換マップ [2-340](#)
  - DTP [2-783](#)
  - DTP ネゴシエーション [2-785](#)
  - DTP フラップ
    - エラー回復タイマー [2-172](#)
    - エラー検出 [2-166](#)
  - duplex コマンド [2-164](#)
  - dynamic auto VLAN メンバーシップ モード [2-782](#)
  - dynamic desirable VLAN メンバーシップ モード [2-782](#)
  - Dynamic Host Configuration Protocol (DHCP)
    - 「DHCP スヌーピング」を参照
  - Dynamic Trunking Protocol (ダイナミック トランッキング プロトコル)
    - 「DTP」を参照
- 
- ## E
- EAP-Request/Identity フレーム
    - 再送信するまでの時間 [2-161](#)
    - 送信する最高回数 [2-153](#)
  - errdisable detect cause small-frame コマンド [2-169](#)
  - errdisable detect cause コマンド [2-166](#)
  - errdisable recovery cause small-frame [2-171](#)
  - errdisable recovery コマンド [2-172](#)
  - errdisable インターフェイス、表示 [2-539](#)
  - errdisable 検出 [2-166](#)
  - EtherChannel
    - EtherChannel/PAgP のデバッグ、表示 [B-14](#)
    - LACP
      - channel-group 情報のクリア [2-96](#)
      - システム プライオリティ [2-281](#)
      - デバッグ メッセージ、表示 [B-22](#)
      - 表示 [2-597](#)

プロトコルの制限 [2-79](#)

ホットスタンバイ ポートのポート プライオリティ [2-279](#)

モード [2-75](#)

## PAgP

channel-group 情報のクリア [2-100](#)

エラー回復タイマー [2-172](#)

エラー検出 [2-166](#)

学習方式 [2-389](#)

集約ポート ラーナー [2-389](#)

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 [2-391](#)

デバッグ メッセージ、表示 [B-32](#)

表示 [2-653](#)

物理ポート ラーナー [2-389](#)

モード [2-75](#)

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 [2-75](#)

インターフェイス情報、表示 [2-539](#)

表示 [2-529](#)

負荷分散方式 [2-407](#)

プラットフォーム特定イベントのデバッグ、表示 [B-40](#)

ポート チャンネル論理インターフェイスの作成 [2-184](#)

exception crashinfo コマンド [2-175](#)

## F

facility alarm status、表示 [2-532](#)

fallback profile コマンド [2-176](#)

fcs-threshold コマンド [2-178](#)

FCS ヒステリシスしきい値 [2-10](#)

FCS ビット エラー率

設定 [2-178](#)

表示 [2-535](#)

変動しきい値 [2-10](#)

fixup コマンド [2-179](#)

flash\_init (ブートローダ) コマンド [A-10](#)

Flex Link

設定 [2-776](#)

表示 [2-539](#)

優先 VLAN の設定 [2-778](#)

flowcontrol コマンド [2-180](#)

format (ブートローダ) コマンド [A-11](#)

fsck (ブートローダ) コマンド [A-12](#)

## H

help (ブートローダ) コマンド [A-13](#)

Hot Standby Router Protocol (ホットスタンバイ ルータ プロトコル)

「HSRP」を参照

HSRP

HSRP グループのクラスタへのバインド [2-119](#)

スタンバイ グループ [2-119](#)

## I

IEEE 802.1x

違反エラーの回復 [2-172](#)

スイッチポート モード [2-783](#)

「ポートベースの認証」も参照

IEEE 802.1x 対応ポートの再認証 [2-157](#)

IEEE 802.1x ポート ベース認証

ゲスト VLAN のサブリカントのイネーブル化 [2-133](#), [2-144](#), [2-177](#)

IGMP グループ、最大値の設定 [2-226](#)

IGMP 最大グループ、デバッグ [B-19](#)

IGMP スヌーピング

querier [2-234](#)

イネーブル化 [2-230](#)

インターフェイスのトポロジ変更通知動作 [2-240](#)

クエリー要求 [2-238](#)

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 [2-244](#)

スイッチのトポロジ変更通知動作 [2-238](#)

設定可能脱退タイマーのイネーブル化 [2-232](#)

即時脱退機能のイネーブル化 [2-241](#)

- 表示 [2-563](#)
- フラッディング クエリー カウント [2-238](#)
- レポート抑制 [2-236](#)
- IGMP フィルタ
  - 適用 [2-225](#)
  - デバッグ メッセージ、表示 [B-18](#)
- IGMP プロファイル
  - 作成 [2-228](#)
  - 表示 [2-562](#)
- inside from コマンド [2-182](#)
- interface port-channel コマンド [2-184](#)
- interface range コマンド [2-186](#)
- Internet Group Management Protocol (インターネットグループ管理プロトコル)
  - 「IGMP」を参照
- ip access-group コマンド [2-188](#)
- ip address コマンド [2-191](#)
- ip admission name proxy http コマンド [2-194](#)
- ip admission コマンド [2-193](#)
- ip arp inspection filter vlan コマンド [2-196](#)
- ip arp inspection limit コマンド [2-198](#)
- ip arp inspection log-buffer コマンド [2-200](#)
- ip arp inspection trust コマンド [2-202](#)
- ip arp inspection validate コマンド [2-204](#)
- ip arp inspection vlan logging コマンド [2-207](#)
- ip arp inspection vlan コマンド [2-206](#)
- ip dhcp snooping binding コマンド [2-210](#)
- ip dhcp snooping database コマンド [2-212](#)
- ip dhcp snooping information option allow-untrusted コマンド [2-216](#)
- ip dhcp snooping information option format remote-id コマンド [2-218](#)
- ip dhcp snooping information option コマンド [2-214](#)
- ip dhcp snooping limit rate コマンド [2-219](#)
- ip dhcp snooping trust コマンド [2-220](#)
- ip dhcp snooping verify コマンド [2-221](#)
- ip dhcp snooping vlan information option format-type circuit-id string コマンド [2-223](#)
- ip dhcp snooping vlan コマンド [2-222](#)
- ip dhcp snooping コマンド [2-209](#)
- 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 [2-225](#)
- ip igmp max-groups コマンド [2-226](#), [2-249](#)
- ip igmp profile コマンド [2-228](#)
- ip igmp snooping last-member-query-interval コマンド [2-232](#)
- ip igmp snooping querier コマンド [2-234](#)
- ip igmp snooping report-suppression コマンド [2-236](#)
- ip igmp snooping tcn flood コマンド [2-240](#)
- ip igmp snooping tcn コマンド [2-238](#)
- ip igmp snooping vlan immediate-leave コマンド [2-241](#)
- ip igmp snooping vlan mrouter コマンド [2-242](#)
- ip igmp snooping vlan static コマンド [2-244](#)
- ip igmp snooping コマンド [2-230](#)
- IP Phone
  - auto-QoS の設定 [2-60](#)
  - 送信されたパケットを信頼する [2-366](#)
- IP Precedence/DSCP マップ [2-340](#)
- ip source binding コマンド [2-246](#)
- ip ssh コマンド [2-248](#)
- ipv6 address dhcp コマンド [2-253](#)
- ipv6 dhcp client request vendor コマンド [2-254](#)
- ipv6 dhcp ping packets コマンド [2-255](#)
- ipv6 dhcp pool コマンド [2-257](#)
- ipv6 dhcp server コマンド [2-260](#)
- ipv6 mld snooping last-listener-query count コマンド [2-264](#)
- ipv6 mld snooping last-listener-query-interval コマンド [2-266](#)
- ipv6 mld snooping listener-message-suppression コマンド [2-268](#)
- ipv6 mld snooping robustness-variable コマンド [2-269](#)
- ipv6 mld snooping tcn コマンド [2-271](#)
- ipv6 mld snooping vlan コマンド [2-273](#)
- ipv6 mld snooping コマンド [2-262](#)
- IPv6 SDM テンプレート [2-452](#)
- ip verify source コマンド [2-251](#)
- IP アドレス、設定 [2-191](#)
- IP アドレスの照合 [2-326](#)

## IP 送信元ガード

イネーブル化 [2-251](#)スタティック IP 送信元バインディング [2-246](#)ディセーブル化 [2-251](#)

表示

ダイナミック バインディング エントリ専用 [2-555](#)バインディング エントリ [2-571](#)

## IP ソース ガード

表示する

設定 [2-572](#)IP マルチキャスト アドレス [2-374](#)

## L

l2nat instance コマンド [2-277](#)l2nat コマンド [2-275](#)

## LACP

「EtherChannel」を参照

lacp port-priority コマンド [2-279](#)lacp system-priority コマンド [2-281](#)

## Link Aggregation Control Protocol

「EtherChannel」を参照

link-diag error-rate コマンド [2-283](#)link state group コマンド [2-284](#)link state track コマンド [2-286](#)location (インターフェイス コンフィギュレーション) コマンド [2-289](#)location (グローバル コンフィギュレーション) コマンド [2-287](#)logging event power-inline-status コマンド [2-292](#)logging event コマンド [2-291](#)logging file コマンド [2-293](#)

## M

mab request format attribute 32 コマンド [2-295](#)mac access-group コマンド [2-297](#)mac access-list extended コマンド [2-299](#)mac address-table aging-time [2-297](#)mac address-table aging-time コマンド [2-301](#)mac address-table learning コマンド [2-302](#)mac address-table move update コマンド [2-304](#)mac address-table notification コマンド [2-306](#)mac address-table static drop コマンド [2-309](#)mac address-table static コマンド [2-308](#)macro apply コマンド [2-311](#)

macro description

定義済み [2-317](#)macro description コマンド [2-314](#), [2-317](#)macro global description コマンド [2-323](#)macro global コマンド [2-320](#)macro name コマンド [2-324](#)MAC アクセス リスト [2-127](#)MAC アクセス リスト コンフィギュレーション モード [2-299](#)

## MAC アドレス

MAC アドレス通知トラップのイネーブル化 [2-306](#)MAC アドレステーブル移行更新のイネーブル化 [2-304](#)VLAN ごとの MAC アドレス ラーニングのディセーブル化 [2-302](#)照合 [2-326](#)

スタティック

インターフェイス上でドロップ [2-309](#)追加および削除 [2-308](#)表示 [2-623](#)テーブル [2-609](#)

動的

エージング タイム [2-301](#)削除 [2-97](#)表示 [2-615](#)

表示

MAC アドレス テーブル移行更新 [2-620](#)VLAN 単位 [2-625](#)VLAN のアドレス数 [2-613](#)インターフェイス単位 [2-617](#)エージング タイム [2-611](#)スタティック [2-623](#)

スタティック エントリおよびダイナミック エントリ [2-607](#)

すべて [2-609](#)

通知設定 [2-619, 2-621](#)

動的 [2-615](#)

MAC アドレス通知、デバッグ [B-24](#)

match (アクセス マップ コンフィギュレーション) コマンド [2-326](#)

match (クラスマップ コンフィギュレーション) コマンド [2-328](#)

mdix auto コマンド [2-330](#)

media--type コマンド [2-331](#)

memory (ブートローダ) コマンド [A-14](#)

mkdir (ブートローダ) コマンド [A-15](#)

MLD スヌーピング

イネーブル化 [2-262](#)

クエリーの設定 [2-264, 2-266](#)

設定 [2-268, 2-269](#)

トポロジ変更通知の設定 [2-271](#)

表示 [2-579, 2-581, 2-585](#)

mls qos aggregate-policer コマンド [2-334](#)

mls qos cos コマンド [2-336](#)

mls qos dscp-mutation コマンド [2-338](#)

mls qos map コマンド [2-340](#)

mls qos queue-set output buffers コマンド [2-344](#)

mls qos queue-set output threshold コマンド [2-346](#)

mls qos rewrite ip dscp コマンド [2-348](#)

mls qos srr-queue input bandwidth コマンド [2-350](#)

mls qos srr-queue input buffers コマンド [2-352](#)

mls qos srr-queue input cos-map コマンド [2-354](#)

mls qos srr-queue input dscp-map コマンド [2-356](#)

mls qos srr-queue input priority-queue コマンド [2-358](#)

mls qos srr-queue input threshold コマンド [2-360](#)

mls qos srr-queue output cos-map コマンド [2-362](#)

mls qos srr-queue output dscp-map コマンド [2-364](#)

mls qos trust コマンド [2-366](#)

mls qos vlan-based コマンド [2-368](#)

mls qos コマンド [2-332](#)

monitor session コマンド [2-369](#)

more (ブートローダ) 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 [2-734](#)

VLAN とインスタンス間のマッピング [2-734](#)

現在または保留中の構成の表示 [2-734](#)

コンフィギュレーション リビジョン番号 [2-734](#)

設定名 [2-734](#)

表示 [2-678](#)

変更の中止 [2-734](#)

変更の適用 [2-734](#)

ステート情報の表示 [2-677](#)

ステート変更

BPDU ガードのイネーブル化 [2-721, 2-750](#)

BPDU フィルタリングのイネーブル化 [2-719, 2-750](#)

PortFast 対応ポートのシャットダウン [2-750](#)

Port Fast のイネーブル化 [2-750, 2-753](#)

転送遅延時間 [2-738](#)

フォワーディング ステートへの高速移行 [2-729](#)

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 [2-753](#)

リスニングおよびラーニング ステートの期間 [2-738](#)

相互運用 [2-106](#)

パス コスト [2-736](#)

表示 [2-678](#)

プロトコル移行プロセスの再開 [2-106](#)

プロトコル モード [2-733](#)

リンク タイプ [2-729](#)

ルート スイッチ

BPDU ドロップまでの最大ホップ数 [2-741](#)

BPDU メッセージの間隔 [2-740](#)

hello BPDU メッセージの間隔 [2-739, 2-746](#)

hello タイム [2-739, 2-746](#)

拡張システム ID の影響 [2-726](#)

スイッチのプライオリティ [2-745](#)

選択に関するポート プライオリティ [2-742](#)

プライマリまたはセカンダリ [2-746](#)

有効期限 [2-740](#)

ルート ポート

指定ポートの制限 [2-727](#)

ルート ガード [2-727](#)

ルートとなるポートの制限 [2-727](#)

ループ ガード [2-727](#)

MTU

グローバル設定の表示 [2-685](#)

サイズの設定 [2-803](#)

Multicast Listener Discovery

「MLD」を参照

Multicast Listener Discovery

「MLD」を参照

Multicast VLAN、MVR [2-375](#)

Multicast VLAN Registration

「MVR」を参照

MVR

アドレスのエイリアス [2-375](#)

インターフェイス情報の表示 [2-645](#)

インターフェイスの設定 [2-377](#)

設定 [2-374](#)

デバッグ メッセージ、表示 [B-29](#)

表示 [2-643](#)

メンバー、表示 [2-647](#)

mvr vlan group コマンド [2-378](#)

mvr (インターフェイス コンフィギュレーション) コマンド [2-377](#)

mvr (グローバル コンフィギュレーション) コマンド [2-374](#)

## N

network-policy profile (ネットワークポリシー コンフィギュレーション) コマンド [2-383](#)

network-policy (グローバル コンフィギュレーション) コマンド [2-381](#)

network-policy コマンド [2-380](#)

nmsp attachment suppress コマンド [2-386](#)

nmsp コマンド [2-385](#)

nonegotiate、速度 [2-761](#)

notifies コマンド [2-17](#)

no vlan コマンド [2-819](#)

NVRAM

バッファ サイズの表示 [2-486](#)

バッファ サイズの変更 [2-65](#)

## O

outside from コマンド [2-387](#)

## P

PAgP

「EtherChannel」を参照

pagp learn-method コマンド [2-389](#)

pagp port-priority コマンド [2-391](#)

permit (ARP アクセス リスト コンフィギュレーション) コマンド [2-393](#)

permit (config-l2nat コンフィギュレーション) コマンド [2-395](#)

permit (MAC アクセス リスト コンフィギュレーション) コマンド [2-397](#)

Per-VLAN Spanning-Tree Plus

「STP」を参照

PID の表示 [2-549](#)

PIM-DVMRP、マルチキャスト ルータ学習方式 [2-242](#)

PoE

コントローラ レジスタ値の表示 [2-508](#)

状態のロギング [2-292](#)

電力管理情報の表示 [2-661](#)

電力管理モードの設定 [2-409](#)

電力設定 [2-412](#)

police aggregate コマンド [2-402](#)

police コマンド [2-400](#)

policy-map コマンド [2-404](#)

Port Aggregation Protocol

「EtherChannel」を参照

port-channel load-balance コマンド [2-407](#)

PortFast、スパニングツリー用 [2-753](#)

power inline consumption コマンド [2-412](#)

Power over Ethernet

「PoE」を参照

power-supply dual コマンド [2-416](#)

priority-queue コマンド [2-417](#)

profinet [2-419](#)

psp [2-421](#)

psp コマンド [2-421](#)

ptp インターフェイス コンフィギュレーション コマンド [2-425](#)

ptp (グローバル コンフィギュレーション) コマンド [2-423](#)

PTP 設定 [2-425](#)

PTP ポート

表示 [2-670](#)

「PTP」を参照 [2-425](#)

PVST+

「STP」を参照

## Q

QoS

auto-QoS

設定 [2-60](#)

デバッグ メッセージ、表示 [B-4](#)

DSCP 透過 [2-348](#)

DSCP の信頼できるポート

DSCP/DSCP 変換マップの定義 [2-340](#)

DSCP/DSCP 変換マップの適用 [2-338](#)

IP Phone の信頼される境界 [2-366](#)

VLAN ベース [2-368](#)

イネーブル化 [2-332](#)

キュー、緊急キューのイネーブル化 [2-417](#)

クラス マップ

一致基準の定義 [2-328](#)

作成 [2-85](#)

表示 [2-492](#)

自動 QoS

表示 [2-480](#)

出力キュー

CoS 値のキューおよびしきい値へのマッピング [2-362](#)

CoS 出力キューのしきい値マップの定義 [2-362](#)

CoS 出力キューのしきい値マップの表示 [2-635](#)

DSCP 値のキューおよびしきい値へのマッピング [2-364](#)

DSCP 出力キューしきい値マップの定義 [2-364](#)

DSCP 出力キューのしきい値マップの表示 [2-635](#)

WTD しきい値の設定 [2-346](#)

キューイングの方針の表示 [2-631](#)

キューセットの表示 [2-638](#)

最大および予約済みメモリ割り当ての設定 [2-346](#)

帯域幅共有とスケジューリングの有効化 [2-767](#)

帯域幅シェーピングとスケジューリングの有効化 [2-765](#)

バッファの割り当て [2-344](#)

バッファ割り当ての表示 [2-631](#)

ポートでの最大出力の制限 [2-763](#)

ポートのキューセットへのマッピング [2-414, 2-427](#)

設定情報の表示 [2-480, 2-627](#)

着信パケットの CoS 値の定義 [2-336](#)

統計情報

キューに入れられた、または削除されたパケット [2-631](#)

送受信した CoS 値 [2-631](#)

送受信した DSCP 値 [2-631](#)

プロファイル内外のパケット [2-631](#)

入力キュー

CoS 値のキューおよびしきい値へのマッピング [2-354](#)

CoS 入力キューのしきい値マップの定義 [2-354](#)

CoS 入力キューのしきい値マップの表示 [2-635](#)

DSCP 値のキューおよびしきい値へのマッピング [2-356](#)

DSCP 入力キューしきい値マップの定義 [2-356](#)

DSCP 入力キューのしきい値マップの表示 [2-635](#)

SRR スケジューリングの重みの割り当て [2-350](#)

WTD しきい値の設定 [2-360](#)

キューイングの方針の表示 [2-631](#)

設定の表示 [2-629](#)

バッファの割り当て [2-352](#)

バッファ割り当ての表示 [2-631](#)

プライオリティ キューのイネーブル化 [2-358](#)

ポートの信頼状態 [2-366](#)

ポリシー マップ

- DSCP 値または IP precedence 値の設定 [2-460](#)
- インターフェイスへの適用 [2-457, 2-462](#)
- 階層 [2-405](#)
- 作成 [2-404](#)
- 集約ポリサーの適用 [2-402](#)
- 信頼状態 [2-812](#)
- トラフィックの分類 [2-83](#)
- ポリサーの定義 [2-334, 2-400](#)
- ポリサーの表示 [2-628](#)
- ポリシー マップの表示 [2-658](#)
- ポリシング設定 DSCP マップ [2-340](#)

マップ

- 定義 [2-340, 2-354, 2-356, 2-362, 2-364](#)
- 表示 [2-635](#)

QoS のポートの信頼状態 [2-366](#)

Quality Of Service

「QoS」を参照

queue-set コマンド [2-414, 2-427](#)

## R

radius-server dead-criteria コマンド [2-428](#)

radius-server host コマンド [2-430](#)

Rapid Per-VLAN Spanning-Tree Plus

「STP」を参照

Rapid PVST+

「STP」を参照

rcommand コマンド [2-432](#)

relay-major コマンド [2-17](#)

relay-minor コマンド [2-17](#)

remote-span コマンド [2-434](#)

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) コマンド [A-17](#)

renew ip dhcp snooping database コマンド [2-436](#)

rep admin vlan コマンド [2-438](#)

rep block port コマンド [2-439](#)

rep lsl-age-timer コマンド [2-442](#)

rep preempt delay コマンド [2-444](#)

rep preempt segment コマンド [2-445](#)

rep segment コマンド [2-446](#)

rep stcn コマンド [2-449](#)

reset (ブートローダ) コマンド [A-18](#)

rmdir (ブートローダ) コマンド [A-19](#)

rmon collection stats コマンド [2-451](#)

RSPAN

- remote-span コマンド [2-434](#)
- RSPAN トラフィックのフィルタリング [2-369](#)
- セッション
- 表示 [2-641](#)
- 設定 [2-369](#)
- 表示 [2-641](#)

## S

sdflash

- 情報の表示 [C-30](#)

sdm prefer コマンド [2-452](#)

SDM テンプレート

- デュアル IPv4 および IPv6 [2-452](#)
- 表示 [2-674](#)

service password-recovery コマンド [2-455](#)

service-policy コマンド [2-457](#)

setup express コマンド [2-465](#)

setup コマンド [2-462](#)

set コマンド [2-460](#)

set (ブートローダ) コマンド [A-20](#)

- show access-lists コマンド [2-467](#)
- show alarm description port [2-470](#)
- show alarm description port コマンド [2-470](#)
- show alarm profile コマンド [2-471](#)
- show alarm settings コマンド [2-473](#)
- show archive status コマンド [2-474](#)
- show arp access-list コマンド [2-475](#)
- show authentication コマンド [2-476](#)
- show auto qos コマンド [2-480](#)
- show boot buffersize コマンド [2-486](#)
- show boot コマンド [2-484](#)
- show cable-diagnostics tdr コマンド [2-487](#)
- show cisp コマンド [2-491](#)
- show class-map コマンド [2-492](#)
- show cluster candidates コマンド [2-495](#)
- show cluster members コマンド [2-497](#)
- show cluster コマンド [2-493](#)
- show controllers cpu-interface コマンド [2-499](#)
- show controllers ethernet-controller コマンド [2-501](#)
- show controllers power inline コマンド [2-508](#)
- show controllers tcam コマンド [2-510](#)
- show controller utilization コマンド [2-512](#)
- show dot1x コマンド [2-514](#)
- show dtp コマンド [2-518](#)
- show eap コマンド [2-520](#)
- show env コマンド [2-522, 2-523](#)
- show errdisable detect コマンド [2-524](#)
- show errdisable flap-values コマンド [2-526](#)
- show errdisable recovery コマンド [2-527](#)
- show etherchannel コマンド [2-529](#)
- show facility-alarm status コマンド [2-532](#)
- show fallback profile コマンド [2-533](#)
- show fcs threshold コマンド [2-535](#)
- show flowcontrol コマンド [2-537](#)
- show interface rep コマンド [2-547](#)
- show interfaces counters コマンド [2-545](#)
- show interfaces rep コマンド [2-547](#)
- show interfaces コマンド [2-539](#)
- show inventory コマンド [2-549](#)
- show ip arp inspection コマンド [2-550](#)
- show ipc コマンド [2-574](#)
- show ip dhcp snooping binding コマンド [2-555](#)
- show ip dhcp snooping database コマンド [2-557, 2-559](#)
- show ip dhcp snooping コマンド [2-554](#)
- show ip igmp profile コマンド [2-562](#)
- show ip igmp snooping address コマンド [2-581](#)
- show ip igmp snooping groups コマンド [2-566](#)
- show ip igmp snooping mrouter コマンド [2-568, 2-583](#)
- show ip igmp snooping querier コマンド [2-569, 2-585](#)
- show ip igmp snooping コマンド [2-563, 2-579](#)
- show ip source binding コマンド [2-571](#)
- show ipv6 dhcp conflict コマンド [2-578](#)
- show ipv6 route updated [2-587](#)
- show ip verify source コマンド [2-572](#)
- show l2nat instance コマンド [2-589](#)
- show l2nat interface コマンド [2-590](#)
- show l2nat statistics interface コマンド [2-595](#)
- show l2nat statistics コマンド [2-592](#)
- show lacp コマンド [2-597](#)
- show link-diag error-rate コマンド [2-601](#)
- show link state group コマンド [2-604](#)
- show location [2-602](#)
- show mac access-group コマンド [2-606](#)
- show mac address-table address コマンド [2-609](#)
- show mac address-table aging time コマンド [2-611](#)
- show mac address-table count コマンド [2-613](#)
- show mac address-table dynamic コマンド [2-615](#)
- show mac address-table interface コマンド [2-617](#)
- show mac address-table learning コマンド [2-619](#)
- show mac address-table move update コマンド [2-620](#)
- show mac address-table notification コマンド [2-98, 2-621, B-26](#)
- show mac address-table static コマンド [2-623](#)
- show mac address-table vlan コマンド [2-625](#)
- show mac address-table コマンド [2-607](#)
- show mls qos aggregate-policer コマンド [2-628](#)
- show mls qos input-queue コマンド [2-629](#)
- show mls qos interface コマンド [2-631](#)

- show mls qos maps コマンド [2-635](#)
- show mls qos queue-set コマンド [2-638](#)
- show mls qos vlan コマンド [2-640](#)
- show mls qos コマンド [2-627](#)
- show monitor コマンド [2-641](#)
- show mvr interface コマンド [2-645](#)
- show mvr members コマンド [2-647](#)
- show mvr コマンド [2-643](#)
- show network-policy profile コマンド [2-649](#)
- show nmsp コマンド [2-650](#)
- show pagp コマンド [2-653](#)
- show parser macro コマンド [2-655](#)
- show platform acl コマンド [C-2](#)
- show platform backup interface コマンド [C-3](#)
- show platform configuration コマンド [C-4](#)
- show platform etherchannel コマンド [C-5](#)
- show platform forward コマンド [C-6](#)
- show platform igmp snooping コマンド [C-8](#)
- show platform ip unicast コマンド [C-9](#)
- show platform ipv6 unicast コマンド [C-14](#)
- show platform ip wccp コマンド [C-13](#)
- show platform layer4op コマンド [C-16](#)
- show platform mac-address-table コマンド [C-17](#)
- show platform messaging コマンド [C-18](#)
- show platform monitor コマンド [C-19](#)
- show platform mvr table コマンド [C-20](#)
- show platform pm コマンド [C-21](#)
- show platform port-asic コマンド [C-22](#)
- show platform port-security コマンド [C-26](#)
- show platform qos コマンド [C-27](#)
- show platform resource-manager コマンド [C-28](#)
- show platform sflash コマンド [C-30](#)
- show platform snmp counters コマンド [C-31](#)
- show platform spanning-tree コマンド [C-32](#)
- show platform stp-instance コマンド [C-33](#)
- show platform team コマンド [C-34](#)
- show platform vlan コマンド [C-36](#)
- show policy-map コマンド [2-658](#)
- show port security コマンド [2-659](#)
- show power inline コマンド [2-661](#)
- show profinet [2-661](#)
- show profinet コマンド [2-663](#)
- show psp config コマンド [2-665](#)
- show psp statistics コマンド [2-666](#)
- show ptp port コマンド [2-670](#)
- show ptp コマンド [2-667, 2-670](#)
- show rep topology コマンド [2-671](#)
- show sdm prefer コマンド [2-674](#)
- show setup express コマンド [2-676](#)
- show spanning-tree コマンド [2-677](#)
- show storm-control コマンド [2-683](#)
- show system mtu コマンド [2-685](#)
- show trust コマンド [2-812](#)
- show udld コマンド [2-686](#)
- show version コマンド [2-689](#)
- show vlan access-map コマンド [2-695](#)
- show vlan filter コマンド [2-696](#)
- show vlan コマンド [2-691](#)
- show vlan コマンド、フィールド [2-693](#)
- show vmps コマンド [2-697](#)
- show vtp コマンド [2-699](#)
- shutdown vlan コマンド [2-705](#)
- shutdown コマンド [2-704](#)
- small violation-rate コマンド [2-706](#)
- Smartports マクロ
  - 「マクロ」を参照
- snmp-server enable traps コマンド [2-708](#)
- snmp-server host コマンド [2-713](#)
- snmp trap mac-notification change コマンド [2-716](#)
- SNMP 通知、送信のイネーブル [2-708](#)
- SNMP トラップ
  - MAC アドレス通知機能のイネーブル化 [2-306](#)
  - MAC アドレス通知トラップのイネーブル化 [2-716](#)
  - 送信のイネーブル化 [2-708](#)
- SNMP ホスト、指定 [2-713](#)
- SoftPhone
  - 「Cisco SoftPhone」を参照
- SPAN

- SPAN トラフィックのフィルタリング **2-369**
  - セッション
    - インターフェイスへの追加 **2-369**
    - 新規に開始 **2-369**
    - 表示 **2-641**
  - 設定 **2-369**
  - デバッグ メッセージ、表示 **B-27**
  - 表示 **2-641**
- spanning-tree backbonefast コマンド **2-718**
- spanning-tree bpdufilter コマンド **2-719**
- spanning-tree bpduguard コマンド **2-721**
- spanning-tree cost コマンド **2-723**
- spanning-tree etherchannel コマンド **2-725**
- spanning-tree extend system-id コマンド **2-726**
- spanning-tree guard コマンド **2-727**
- spanning-tree link-type コマンド **2-729**
- spanning-tree loopguard default コマンド **2-731**
- spanning-tree mode コマンド **2-733**
- spanning-tree mst configuration コマンド **2-734**
- spanning-tree mst cost コマンド **2-736**
- spanning-tree mst forward-time コマンド **2-738**
- spanning-tree mst hello-time コマンド **2-739**
- spanning-tree mst max-age コマンド **2-740**
- spanning-tree mst max-hops コマンド **2-741**
- spanning-tree mst port-priority コマンド **2-742**
- spanning-tree mst pre-standard コマンド **2-744**
- spanning-tree mst priority コマンド **2-745**
- spanning-tree mst root コマンド **2-746**
- 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 **2-753**
- spanning-tree portfast (グローバル コンフィギュレーション) コマンド **2-750**
- spanning-tree port-priority コマンド **2-748**
- spanning-tree transmit hold-count コマンド **2-755**
- spanning-tree uplinkfast コマンド **2-756**
- spanning-tree vlan コマンド **2-758**
- speed コマンド **2-761**
- srr-queue bandwidth limit コマンド **2-763**
- srr-queue bandwidth share コマンド **2-767**
- SSH、バージョンの設定 **2-248**
- storm-control コマンド **2-769**
- STP
  - BackboneFast **2-718**
  - EtherChannel の設定矛盾 **2-725**
  - VLAN オプション **2-745, 2-758**
  - カウンタ、クリア **2-105**
  - 拡張システム ID **2-726**
  - 間接リンク障害の検出 **2-718**
  - ステート情報の表示 **2-677**
  - ステート変更
    - BPDU ガードのイネーブル化 **2-721, 2-750**
    - BPDU フィルタリングのイネーブル化 **2-719, 2-750**
    - PortFast 対応ポートのシャットダウン **2-750**
    - Port Fast のイネーブル化 **2-750, 2-753**
    - エラー ステートから回復するタイマーのイネーブル化 **2-172**
    - 転送遅延時間 **2-758**
    - 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 **2-753**
    - リスニングおよびラーニング ステートの期間 **2-758**
- デバッグ メッセージ、表示
  - BackboneFast イベント **B-90**
  - MSTP **B-93**
  - UplinkFast **B-97**
  - 最適化された BPDU 処理 **B-92**
  - スイッチ シム **B-95**
  - スパニングツリーのアクティビティ **B-88**
  - 送受信された BPDU **B-91**
- パス コスト **2-723**
- プロトコル モード **2-733**
- ルート スイッチ
  - BPDU メッセージの間隔 **2-758**
  - hello BPDU メッセージの間隔 **2-758**
  - hello タイム **2-758**
  - 拡張システム ID の影響 **2-726, 2-759**
  - スイッチのプライオリティ **2-758**
  - 選択に関するポート プライオリティ **2-748**

プライマリまたはセカンダリ **2-758**  
 有効期限 **2-758**  
 ルート ポート  
 UplinkFast **2-756**  
 新しいルート ポート選択の高速化 **2-756**  
 指定ポートの制限 **2-727**  
 ルート ガード **2-727**  
 ルートとなるポートの制限 **2-727**  
 ループ ガード **2-727**  
 STP の拡張システム ID **2-726**  
 SVI ステータスの計算 **2-774**  
 switchport access コマンド **2-772**  
 switchport autostate exclude コマンド **2-774**  
 switchport backup interface コマンド **2-776**  
 switchport block コマンド **2-780**  
 switchport host コマンド **2-781**  
 switchport mode コマンド **2-782**  
 switchport nonegotiate コマンド **2-785**  
 switchport port-security aging コマンド **2-792**  
 switchport port-security コマンド **2-787**  
 switchport priority extend コマンド **2-794**  
 switchport protected コマンド **2-796**  
 switchport trunk コマンド **2-797**  
 switchport voice vlan コマンド **2-800**  
 SYN  
 ファイルの除外 **2-802**  
 フラッシュ **2-802**  
 古いファイルの格納 **2-802**  
 sync flash sdflash コマンド **2-802**  
 syslog コマンド **2-17**  
 system mtu コマンド **2-803**

## T

tar ファイル、作成、一覧表示、および抽出 **2-25**  
 TDR、実行 **2-805**  
 Telnet、クラスタ スイッチへの通信に使用 **2-432**  
 test cable-diagnostics tdr コマンド **2-805**  
 test relay コマンド **2-806**

traceroute mac ip コマンド **2-810**  
 traceroute mac コマンド **2-807**  
 type (ブートローダ) コマンド **A-23**

## U

### UDLD

アグレッシブ モード **2-814, 2-816**  
 インターフェイスごとのイネーブル化 **2-816**  
 エラー回復タイマー **2-172**  
 グローバルにイネーブル化 **2-814**  
 シャットダウン インターフェイスのリセット **2-818**  
 ステータス **2-686**  
 デバッグ メッセージ、表示 **B-104**  
 ノーマル モード **2-814, 2-816**  
 メッセージ タイマー **2-814**  
 udld port コマンド **2-816**  
 udld reset コマンド **2-818**  
 udld コマンド **2-814**  
 UniDirectional Link Detection (単方向リンク検出)  
 「UDLD」を参照  
 unset (ブートローダ) コマンド **A-25**  
 UplinkFast、STP 用 **2-756**

## V

version (ブートローダ) コマンド **A-27**

### VLAN

#### MAC アドレス

数 **2-613**

表示 **2-625**

VTP の SNMP トラップ **2-711**

拡張範囲 **2-819**

ゲスト VLAN のサブリカントのイネーブル化 **2-133, 2-144, 2-177**

再起動 **2-705**

シャットダウン **2-705**

設定 **2-819**

- 設定の表示 [2-691](#)
- 設定の保存 [2-819](#)
- 中断 [2-705](#)
- 追加 [2-819](#)
- デバッグ メッセージ、表示
  - ISL [B-101](#)
  - VLAN IOS File System エラー テスト [B-100](#)
  - VLAN マネージャのアクティビティ [B-98](#)
  - VTP [B-102](#)
- 標準範囲 [2-819](#)
- メディア タイプ [2-822](#)
- vlan access-map コマンド [2-825](#)
- vlan filter コマンド [2-827](#)
- VLAN ID 範囲 [2-819](#)
- VLAN Query Protocol
  - 「VQP」を参照
- VLAN Trunking Protocol
  - 「VTP」を参照
- VLAN アクセス マップ
  - アクション [2-6](#)
  - 表示 [2-695](#)
- VLAN アクセス マップ コンフィギュレーション モード [2-825](#)
- vlan (グローバル コンフィギュレーション) コマンド [2-819](#)
- VLAN コンフィギュレーション モード
  - 開始 [2-819](#)
  - 概要 [1-2](#)
  - 説明 [1-4](#)
- VLAN 設定
  - 保存 [2-820](#)
  - ルール [2-823](#)
- VLAN での MLD スヌーピング、イネーブル化 [2-273](#)
- VLAN トランッキング プロトコル
  - 「VTP」を参照
- VLAN フィルタ、表示 [2-696](#)
- VLAN ベースの QoS [2-368](#)
- VLAN マップ
  - 作成 [2-825](#)
- 定義 [2-326](#)
- 適用 [2-827](#)
- 表示 [2-695](#)
- VMPS
  - エラー回復タイマー [2-173](#)
  - サーバの設定 [2-832](#)
  - ダイナミック VLAN 割り当ての再確認 [2-829](#)
  - 表示 [2-697](#)
- vmps reconfirm (グローバル コンフィギュレーション) コマンド [2-830](#)
- vmps reconfirm (特権 EXEC) コマンド [2-829](#)
- vmps retry コマンド [2-831](#)
- vmps server コマンド [2-832](#)
- VQP
  - クライアント統計情報のクリア [2-108](#)
  - サーバごとの再試行回数 [2-831](#)
  - 再確認間隔 [2-830](#)
  - 情報の表示 [2-697](#)
  - ダイナミック VLAN 割り当ての再確認 [2-829](#)
  - ダイナミック アクセス ポート [2-773](#)
- VTP
  - 設定の保存 [2-820](#)
  - 統計情報 [2-699](#)
  - ポート単位でのイネーブル化 [2-839](#)
- vtp
  - イネーブル化
    - バージョン 2 [2-835](#)
    - プルーニング [2-835](#)
  - カウンタ表示フィールド [2-700](#)
  - 情報の表示 [2-699](#)
  - ステータス [2-699](#)
  - ステータス表示フィールド [2-702](#)
  - 設定
    - ドメイン名 [2-834](#)
    - パスワード [2-835](#)
    - ファイル名 [2-834](#)
    - モード [2-834](#)
  - 特性の変更 [2-834](#)
  - プルーニング [2-835](#)

プルーニング カウンタのクリア [2-109](#)

モード [2-834](#)

vtp primary コマンド [2-840](#)

vtp (インターフェイス コンフィギュレーション) コマンド [2-839](#)

vtp (グローバル コンフィギュレーション) コマンド [2-834](#)

## あ

アクセス グループ

IP [2-188](#)

MAC、表示 [2-606](#)

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 [2-782](#)

アクセス マップ コンフィギュレーション モード [2-326](#)

アクセス モード [2-782](#)

アップグレード

ソフトウェア イメージ

ステータスのモニタリング [2-474](#)

ダウンロード [2-22](#)

アドレスのエイリアス [2-375](#)

アラーム ID [2-18, 2-470](#)

## い

イーサネット コントローラ、内部レジスタの表示 [2-501](#)

イーサネット統計情報、収集 [2-451](#)

イメージ

「ソフトウェア イメージ」を参照

[2-164](#)

インターフェイス

MAC アドレス テーブルの表示 [2-617](#)

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 [2-75](#)

再起動 [2-704](#)

設定 [2-164](#)

ディセーブル化 [2-704](#)

デバッグ メッセージ、表示 [B-15](#)

複数の設定 [2-186](#)

ポート チャネル論理の作成 [2-184](#)

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 [2-761](#)

インターフェイス範囲マクロ [2-122](#)

## え

エラー条件、表示 [2-526](#)

## お

音声 VLAN

設定 [2-800](#)

ポート プライオリティの設定 [2-794](#)

温度アラーム、設定 [2-15](#)

オンライン診断

グローバル コンフィギュレーション モード

ヘルス モニタ診断テスト スケジュールのクリア [2-90](#)

ヘルス モニタ診断テスト スケジュールのセットアップ [2-90](#)

ヘルス モニタ診断テストの設定 [2-90](#)

## か

階層ポリシー マップ [2-405](#)

回復メカニズム

原因 [2-172](#)

タイマーの間隔 [2-173](#)

表示 [2-89, 2-487, 2-524, 2-527](#)

拡張検出、候補スイッチの [2-112](#)

拡張範囲 VLAN

許可 VLAN リスト [2-797](#)

設定 [2-819](#)

ブルーニング適格リスト [2-797](#)

環境アラーム接点

表示 [2-523](#)

環境アラーム、表示 [2-473](#)

環境変数、表示 [2-484](#)

## き

起動

Cisco IOS イメージ [2-74](#)

環境変数の表示 [2-484](#)

手動 [2-72](#)

中断 [2-67](#)

許可 VLAN [2-797](#)

許可ステート、制御ポートの [2-155](#)

## く

クエリー時間、MVR [2-374](#)

クラスタ

HSRP グループのクラスタへのバインド [2-119](#)

HSRP スタンバイ グループ [2-119](#)

SNMP トラップ [2-708](#)

拡張検出のホップ カウント制限 [2-112](#)

候補の追加 [2-115](#)

冗長性 [2-119](#)

通信

Telnet を使用したメンバ [2-432](#)

クラスタの外部にある装置 [2-117](#)

デバッグ メッセージ、表示 [B-9](#)

入力して設定 [2-115](#)

表示

候補スイッチ [2-495](#)

ステータス [2-493](#)

デバッグ メッセージ [B-9](#)

メンバ スイッチ [2-497](#)

クラス マップ

一致基準の定義 [2-328](#)

作成 [2-85](#)

表示 [2-492](#)

クリティカル VLAN [2-37](#)

グローバル コンフィギュレーション モード [1-2, 1-3](#)

## こ

高精度時間プロトコル

候補スイッチ

「クラスタ」を参照

コマンド スイッチ

「クラスタ」を参照

コンフィギュレーション ファイル

名前の指定 [2-65, 2-66, 2-73](#)

パスワード回復のディセーブル時の考慮事項 [A-1](#)

## さ

サービス クラス

「CoS」を参照

最大伝送単位

「MTU」を参照

再認証

試行間隔 [2-161](#)

定期的 [2-158](#)

## し

システム アラーム

設定 [2-8](#)

システム メッセージのログ [2-292](#)

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 [2-293](#)

システム リソース テンプレート [2-452](#)

自動ネゴシエーション、デュプレックス モードの [2-165](#)

ジャンボ フレーム

「MTU」を参照

集約ポート ラーナー [2-389](#)

受信、フロー制御パケットの [2-180](#)

冗長性、クラスタ スイッチの [2-119](#)

信頼される境界、QoS の [2-366](#)

## す

スイッチド ポート アナライザ

「SPAN」を参照

スタティック アクセス ポート、設定 [2-772](#)

スティッキ ラーニング、イネーブル化 [2-787](#)

スパニングツリー プロトコル

「STP」を参照

## せ

制限 VLAN

「dot1x auth-fail vlan」を参照

製品識別情報の表示 [2-549](#)

セカンダリ 温度アラーム [2-15](#)

セキュア ポート、制限 [2-789](#)

設定、複数のインターフェイスの [2-186](#)

## そ

送信、フロー制御パケットの [2-180](#)

送信元ポート、MVR [2-377](#)

即時脱退機能、MVR [2-377](#)

即時脱退処理 [2-241](#)

即時脱退処理、IPv6 [2-273](#)

ソフトウェア イメージ

アップグレード [2-22](#)

アップロード [2-28](#)

削除 [2-124](#)

ダウンロード [2-22](#)

ソフトウェア バージョン、表示 [2-689](#)

## た

ダイナミック ARP インспекション

ARP ACL

VLAN に適用 [2-196](#)

定義 [2-30](#)

パケットの許可 [2-393](#)

パケットの拒否 [2-125](#)

表示 [2-475](#)

clear

統計情報 [2-91](#)

log buffer

configure [2-200](#)

VLAN 単位でイネーブル化 [2-206](#)

インターフェイスの信頼状態 [2-202](#)

エラー検出 [2-166](#)

記録するパケットのタイプ [2-207](#)

クリア

ログ バッファ [2-90](#)

検証チェック [2-204](#)

着信 ARP パケットのレート制限 [2-198](#)

統計情報

クリア [2-91](#)

表示 [2-550](#)

表示

ARP ACL [2-475](#)

信頼状態およびレート制限 [2-550](#)

設定および動作ステート [2-550](#)

統計情報 [2-550](#)

ログ バッファ [2-550](#)

ログ バッファ

クリア [2-90](#)

表示 [2-550](#)

ダイナミック アクセス ポート

制限 [2-773](#)

設定 [2-772](#)

弾力的、認証、順序付け [2-48](#)

## て

定義済みのコマンド モード [1-1](#)

ディレクトリ、削除 [2-124](#)

テストリレー [2-806](#)  
 電源アラーム、設定 [2-12](#)  
 電源装置モード [2-416](#)  
 転送結果の表示 [C-6](#)  
 テンプレート、システムリソース [2-452](#)

---

## と

統計情報、イーサネットグループ [2-451](#)  
 特権 EXEC モード [1-2, 1-3](#)  
 ドメイン名、VTP [2-834](#)  
 トランキング、VLAN モード [2-782](#)  
 トランク、DTP をサポートしないデバイス [2-783](#)  
 トランクポート [2-782](#)  
 トランクモード [2-782](#)

---

## な

内部レジスタ、表示 [2-501, 2-510](#)

---

## に

認証失敗 VLAN  
 「dot1x auth-fail vlan」を参照

---

## ね

ネイティブ VLAN [2-797](#)

---

## は

ハードウェア ACL 統計情報 [2-467](#)  
 パケットの転送、ACL の一致 [2-6](#)  
 パケットのドロップ、ACL の一致 [2-6](#)  
 パスワード、VTP [2-835](#)  
 バックアップ、インターフェイス  
   設定 [2-776](#)  
   表示 [2-539](#)

---

## ひ

非 IP トラフィック アクセス リスト [2-299](#)  
 非 IP トラフィックの転送  
   許可 [2-397](#)  
   拒否 [2-127](#)  
 非 IP プロトコル  
   拒否 [2-127](#)  
   転送 [2-397](#)  
 非ネゴシエーション DTP メッセージング [2-785](#)  
 標準範囲 VLAN [2-819](#)

---

## ふ

ファイル、削除 [2-124](#)  
 ファイル名、VTP [2-834](#)  
 ブートローダ  
   アクセス [A-1](#)  
   環境変数  
     設定 [A-20](#)  
     設定の表示 [A-20](#)  
     説明 [A-20](#)  
     場所 [A-21](#)  
     リセット [A-25](#)  
   起動  
     Cisco IOS イメージ [A-2](#)  
     ヘルパー イメージ [2-69](#)  
   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-4, A-16, A-23](#)
  - 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](#)
  - フォールバック プロファイル、表示 [2-533](#)
  - 負荷分散方式、EtherChannel [2-407](#)
  - 物理ポート ラーナー [2-389](#)
  - 不明なマルチキャスト トラフィック、回避 [2-780](#)
  - 不明なユニキャスト トラフィック、回避 [2-780](#)
  - プライマリ温度アラーム [2-15](#)
  - プルーニング
    - VLAN [2-797](#)
    - VTP
      - イネーブル化 [2-835](#)
      - インターフェイス情報の表示 [2-539](#)
  - プルーニング適格 VLAN リスト [2-798](#)
  - 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 [C-6](#)
  - ブロードキャスト ストーム制御 [2-769](#)
- 
- ## ほ
- ポート セキュリティ
    - イネーブル化 [2-787](#)
    - 違反エラーの回復 [2-172](#)
    - エージング [2-792](#)
    - デバッグ メッセージ、表示 [B-71](#)
  - ポート タイプ、MVR [2-377](#)
  - ポート、デバッグ [B-69](#)
  - ポートの信頼状態、QoS のポート [2-366](#)
  - ポート範囲、定義 [2-122](#)
  - ポート ベース認証
    - IEEE 802.1x 対応ポートの再認証 [2-157](#)
    - 定期的な再認証
      - イネーブル化 [2-158](#)
  - ポートベース認証
    - AAA 方式のリスト [2-3](#)
    - IEEE 802.1x AAA アカウンティング方式 [2-1](#)
    - IEEE 802.1x のイネーブル化
      - インターフェイス単位 [2-155](#)
      - グローバル [2-130](#)
    - IEEE 802.1x の準備テスト [2-159](#)
    - MAC 認証バイパス [2-150](#)
    - 違反モードの設定 [2-163](#)
    - インターフェイスの初期化 [2-149, 2-160](#)
    - オーセンティケータとしての PAE [2-154](#)
    - 許可ステートの手動制御 [2-155](#)
    - ゲスト VLAN [2-145](#)
    - スイッチからクライアントへの再送信時間 [2-161](#)
    - スイッチから認証サーバへの再送信時間 [2-161](#)
    - スイッチとクライアント間のフレーム再送信回数 [2-152 ~ 2-153](#)
    - 設定可能な IEEE 802.1x パラメータのリセット [2-143](#)
  - 定期的な再認証
    - 試行間隔 [2-161](#)
  - デバッグ メッセージ、表示 [B-11](#)
  - 認証交換に失敗したあとの待機期間 [2-161](#)
  - ホスト モード [2-147](#)
- ポート、保護 [2-796](#)
  - ホスト接続、ポート設定 [2-781](#)
  - ホップ カウント制限、クラスタの [2-112](#)
  - ポリシー マップ
    - インターフェイスへの適用 [2-457, 2-462](#)
  - 階層 [2-405](#)
  - 作成 [2-404](#)
  - トラフィックの分類
    - DSCP 値または IP precedence 値の設定 [2-460](#)
    - クラスの定義 [2-83](#)
    - 信頼状態の定義 [2-812](#)
  - 表示 [2-658](#)
  - ポリサー
    - 単一クラス用 [2-400](#)
    - 表示 [2-628](#)

複数のクラス [2-334](#), [2-402](#)

ポリシング設定 DSCP マップ [2-340](#)

ポリシング設定 DSCP マップ [2-340](#)

## ま

### マクロ

global description の追加 [2-323](#)

インターフェイス範囲 [2-122](#), [2-186](#)

作成 [2-324](#)

説明の追加 [2-314](#)

追跡 [2-320](#)

適用 [2-320](#)

パラメータ値の指定 [2-320](#)

表示 [2-655](#)

### マップ

#### QoS

定義 [2-340](#)

表示 [2-635](#)

#### VLAN

作成 [2-825](#)

定義 [2-326](#)

表示 [2-695](#)

マルチキャスト グループ、MVR [2-375](#)

マルチキャスト グループ アドレス、MVR [2-377](#)

マルチキャスト ストーム制御 [2-769](#)

マルチキャスト ルータ 学習方式 [2-242](#)

マルチキャスト ルータ ポート、IPv6 [2-273](#)

マルチキャスト ルータ ポート、設定 [2-242](#)

マルチ スパニングツリー プロトコル

「MSTP」を参照

## む

### 無効な GBIC

エラー回復タイマー [2-172](#)

エラー検出 [2-166](#)

## め

メカニズムの検出、原因 [2-166](#)

メディア タイプ

ライン コンソール [2-331](#)

メンバ スイッチ

「クラスタ」を参照

## も

モード、MVR [2-374](#)

モード、コマンド [1-1](#)

## ゆ

ユーザ EXEC モード [1-2](#), [1-3](#)

ユニキャスト ストーム制御 [2-769](#)

## 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 [2-674](#)

リンクの診断 [2-601](#)

ウィンドウ サイズ [2-283](#)

リンク フラップ

エラー回復タイマー [2-172](#)

エラー検出 [2-166](#)

## る

ルーテッド ポート

IP アドレス [2-192](#)

サポートされる数 [2-192](#)

ルート ガード、スパニングツリー用 [2-727](#)

ループ ガード、スパニングツリー用 [2-727](#), [2-731](#)

ループバック エラー

回復タイマー [2-172](#)

検出 [2-166](#)

---

## れ

レイヤ 2 traceroute

IP アドレス [2-810](#)

MAC アドレス [2-807](#)

レシーバ ポート、MVR [2-377](#)

---

## ろ

論理インターフェイス [2-184](#)



©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>