コマンドリファレンス、Cisco IOS XE Denali 16.3.x（Catalyst 3850 スイッチ）

初版：2016 年 08 月 01 日

最終更新：2017 年 03 月 03 日

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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

© 2016 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xxxv

表記法 xxxv

関連資料 xxxvii

マニュアルの入手方法およびテクニカル サポート xxxvii

コマンドライン インターフェイスの使用 1

コマンドライン インターフェイスの使用 1

コマンド モードについて 1

ヘルプ システムについて 5

コマンドの省略形 5

コマンドの no 形式および default 形式の概要 6

CLI のエラー メッセージについて 6

コンフィギュレーション ロギングの使用方法 7

コマンド履歴の使用 8

コマンド履歴バッファ サイズの変更 8

コマンドの呼び出し 8

コマンド履歴機能の無効化 9

編集機能の使用方法 9

編集機能の有効化および無効化 9

キーストロークによるコマンドの編集 10

画面幅よりも長いコマンドラインの編集 12

show および more コマンド出力の検索およびフィルタリング 13

CLI のアクセス 13

コンソール接続または Telnet による CLI アクセス 14

キャンパス ファブリック コマンド 15

キャンパス ファブリック コマンド 17

border 17

コンテキスト 18
control-plane 19
domain 20
debug fabric auto 21
fabric auto 22
host-pool name 23
show fabric domain 24
show fabric context 25
show fabric host-pool 26
CleanAir 29
CleanAir コマンド 31
ap dot11 5ghz cleanair 32
ap dot11 5ghz cleanair alarm air-quality 33
ap dot11 5ghz cleanair alarm device 34
default ap dot11 5ghz cleanair device 35
ap dot11 5ghz rrm channel cleanair-event 36
ap dot11 5ghz rrm channel device 38
ap dot11 24ghz cleanair 39
ap dot11 24ghz cleanair alarm air-quality 40
ap dot11 24ghz cleanair alarm device 41
default ap dot11 24ghz cleanair device 42
ap dot11 24ghz rrm channel cleanair-event 45
ap dot11 24ghz rrm channel device 46
ap name mode se-connect 47
default ap dot11 5ghz cleanair device 48
default ap dot11 5ghz rrm channel cleanair-event 49
default ap dot11 5ghz rrm channel device 50
default ap dot11 24ghz cleanair alarm device 51
default ap dot11 24ghz cleanair device 52
default ap dot11 24ghz rrm channel cleanair-event 55
show ap dot11 5ghz cleanair air-quality summary 56
show ap dot11 5ghz cleanair air-quality worst 56
show ap dot11 5ghz cleanair config 57
show ap dot11 5ghz cleanair device type 59
show ap dot11 24ghz cleanair air-quality summary 60

show ap dot11 24ghz cleanair air-quality worst 61
show ap dot11 24ghz cleanair config 61
show ap dot11 24ghz cleanair summary 63
Flexible NetFlow コマンド 65
Flexible NetFlow コマンド 67
cache 69
clear flow exporter 71
clear flow monitor 72
collect 74
collect counter 75
collect interface 76
collect timestamp absolute 77
collect transport tcp flags 79
datalink flow monitor 80
debug flow exporter 81
debug flow monitor 82
debug flow record 83
debug sampler 84
description 85
destination 86
dscp 87
export-protocol netflow-v9 88
exporter 89
フロー エクスポータ 90
フロー モニタ 91
flow record 92
ip flow monitor 93
ipv6 flow monitor 95
match datalink ethertype 96
match datalink mac 98
match datalink vlan 99
match flow cts 100
match flow direction 101
match interface 102
match ipv4 103

match ipv4 destination address 104
match ipv4 source address 105
match ipv4 ttl 106
match ipv6 107
match ipv6 destination address 108
match ipv6 hop-limit 109
match ipv6 source address 110
match transport 111
match transport icmp ipv4 112
match transport icmp ipv6 113
mode random 1 out-of 115
オプション 116
record 117
sampler 118
show flow exporter 120
show flow interface 122
show flow monitor 124
show flow record 129
show sampler 130
source 132
template data timeout 134
transport 135
ttl 136
インターフェイスおよびハードウェア コンポーネント 137
インターフェイスおよびハードウェア コマンド 139
client vlan 141
debug ilpower 142
debug interface 144
debug lldp packets 145
debug nmsp 146
debug platform poe 147
duplex 148
errdisable detect cause 150
errdisable recovery cause 152
errdisable recovery interval 155

interface 156
interface range 157
ip mtu 159
ipv6 mtu 160
lldp（インターフェイス コンフィギュレーション） 161
logging event power-inline-status 163
mdix auto 164
mode（電源スタックの設定） 165
network-policy 167
network-policy profile（グローバル コンフィギュレーション） 168
nmsp attachment suppress 169
power efficient-ethernet auto 170
power-priority 171
power inline 173
power inline police 177
電源装置 179
show CAPWAP summary 181
show controllers cpu-interface 182
show controllers ethernet-controller 183
show controllers utilization 194
show eee 195
show env 199
show errdisable detect 202
show errdisable recovery 204
show interfaces 205
show interfaces counters 209
show interfaces switchport 212
show interfaces transceiver 214
show memory platform 217
show module 219
show mgmt-infra trace messages ilpower 220
show mgmt-infra trace messages ilpower-ha 221
show mgmt-infra trace messages platform-mgr-poe 222
show network-policy profile 223
show platform CAPWAP summary 224

show platform forward 224
show platform hardware fed switch forward 226
show platform resources 229
show platform software ilpower 229
show platform software process list 231
show platform software process slot switch 233
show platform software status control-processor 235
show processes cpu platform monitor 237
show processes memory platform 239
show power inline 242
show stack-power 248
show system mtu 250
show tech-support 251
show wireless interface summary 253
speed 254
stack-power 256
switchport block 257
system mtu 259
test mcu read-register 260
voice-signaling vlan（ネットワークポリシー コンフィギュレーション） 262
voice vlan（ネットワークポリシー コンフィギュレーション） 263
wireless ap-manager interface 265
wireless exclusionlist 266
wireless linktest 267
wireless management interface 268
wireless peer-blocking forward-upstream 268

IP 271

IP コマンド 273

clear ip nhrp 274
debug nhrp 276
fhrp delay 278
fhrp version vrrp v3 279
glbp authentication 280
glbp forwarder preempt 281
glbp ip 282

glbp load-balancing 284
glbp name 285
glbp preempt 287
glbp priority 288
glbp timers 290
glbp weighting 292
glbp weighting track 294
ip address dhcp 296
ip address pool (DHCP) 300
ip address 301
ip nhrp map 304
ip nhrp map multicast 306
ip nhrp network-id 308
ip nhrp nhs 309
key chain 312
key-string（認証） 313
key 314
show glbp 316
show ip nhrp nhs 320
show key chain 323
show track 324
track 326
vrrp 328
vrrp description 329
vrrp preempt 330
vrrp priority 331
vrrp timers advertise 333
vrrs leader 334
IP マルチキャスト ルーティング コマンド 337
IP マルチキャスト コマンド 339
cache-memory-max 340
clear ip mfib counters 341
clear ip mroute 343
ip igmp filter 344
ip igmp max-groups 345

ip igmp profile 347
ip igmp snooping 348
ip igmp snooping last-member-query-count 349
ip igmp snooping querier 351
ip igmp snooping report-suppression 353
ip igmp snooping vlan mrouter 354
ip igmp snooping vlan static 356
ip multicast auto-enable 357
ip multicast vlan 358
ip pim accept-register 359
ip pim bsr-candidate 360
ip pim rp-candidate 362
ip pim send-rp-announce 364
ip pim spt-threshold 365
match message-type 366
match service-type 367
match service-instance 368
mrinfo 369
redistribute mdns-sd 370
service-list mdns-sd 371
service-policy-query 373
service-routing mdns-sd 373
service-policy 374
show ip igmp filter 375
show ip igmp profile 376
show ip igmp snooping 377
show ip igmp snooping groups 379
show ip igmp snooping igmpv2-tracking 380
show ip igmp snooping mrouter 381
show ip igmp snooping querier 382
show ip igmp snooping wireless mcast-spi-count 384
show ip igmp snooping wireless mgid 384
show ip pim autorp 386
show ip pim bsr-router 386
show ip pim bsr 387

show ip pim tunnel 388
show mdns cache 390
show mdns requests 391
show mdns statistics 392
show platform ip multicast 393
wireless mdns-bridging 400
wireless multicast 401

IPv6 403

IPv6 コマンド 405

ipv6 flow monitor 405
ipv6 traffic-filter 406
show wireless ipv6 statistics 407

レイヤ 2/3 409

レイヤ 2/3 コマンド 411

channel-group 412
channel-protocol 416
clear lacp 418
clear pagp 419
clear spanning-tree counters 420
clear spanning-tree detected-protocols 421
debug etherchannel 422
debug lacp 424
debug pagp 425
debug platform pm 426
debug platform udld 428
debug spanning-tree 429
interface port-channel 431
lacp max-bundle 432
lacp port-priority 434
lacp rate 435
lacp system-priority 436
pagp learn-method 437
pagp port-priority 439
port-channel 440
port-channel auto 441

port-channel load-balance 442
port-channel load-balance extended 444
port-channel min-links 445
rep admin vlan 446
rep block port 447
rep lsl-age-timer 449
rep lsl-retries 450
rep preempt delay 450
rep preempt segment 452
rep segment 453
rep stcn 455
show etherchannel 456
show interfaces rep detail 459
show lacp 460
show pagp 464
show platform etherchannel 466
show platform pm 467
show rep topology 468
show udld 470
switchport 474
switchport access vlan 475
switchport mode 477
switchport nonegotiate 480
switchport voice vlan 481
udld 484
udld port 486
udld reset 488

Lightweight アクセス ポイント 491

Cisco Lightweight アクセス ポイント コマンド 493

ap auth-list ap-policy 499
ap bridging 500
ap capwap multicast 501
ap capwap retransmit 502
ap capwap timers 503
ap cdp 505

ap core-dump 506
ap country 507
ap crash-file 508
ap dot11 24ghz preamble 509
ap dot11 24ghz dot11g 510
ap dot11 5ghz channelswitch mode 511
ap dot11 5ghz power-constraint 512
ap dot11 beaconperiod 513
ap dot11 beamforming 514
ap dot11 cac media-stream 515
ap dot11 cac multimedia 517
ap dot11 cac video 519
ap dot11 cac voice 520
ap dot11 cleanair 524
ap dot11 cleanair alarm air-quality 525
ap dot11 cleanair alarm device 525
ap dot11 cleanair device 527
ap dot11 dot11n 528
ap dot11 dtpc 531
ap dot11 edca-parameters 532
ap dot11 rrm group-mode 533
ap dot11 rrm channel cleanair-event 534
ap dot11 l2roam rf-params 535
ap dot11 media-stream 537
ap dot11 rrm ccx location-measurement 538
ap dot11 rrm channel dca 539
ap dot11 rrm group-member 541
ap dot11 rrm logging 542
ap dot11 rrm monitor 543
ap dot11 rrm ndp-type 544
ap dot11 5ghz dot11ac frame-burst 545
ap dot1x max-sessions 546
ap dot1x username 547
ap ethernet duplex 548
ap group 549

ap image 550
ap ipv6 tcp adjust-mss 551
ap led 552
ap link-encryption 553
ap link-latency 553
ap mgmtuser username 554
ap name ap-groupname 556
ap name antenna band mode 557
ap name bhrate 558
ap name bridgegroupname 558
ap name bridging 559
ap name cdp interface 560
ap name console-redirect 561
ap name capwap retransmit 562
ap name command 563
ap name core-dump 564
ap name country 565
ap name crash-file 566
ap name dot11 24ghz rrm coverage 567
ap name dot11 49ghz rrm profile 568
ap name dot11 5ghz rrm channel 570
ap name dot11 antenna 571
ap name dot11 antenna extantgain 572
ap name dot11 cleanair 573
ap name dot11 dot11n antenna 574
ap name dot11 dual-band cleanair 575
ap name dot11 dual-band shutdown 576
ap name dot11 rrm ccx 576
ap name dot11 rrm profile 577
ap name dot11 txpower 579
ap name dot1x-user 580
ap name ethernet 581
ap name ethernet duplex 582
ap name key-zeroize 584
ap name image 584

ap name ipv6 tcp adjust-mss 585
ap name jumbo mtu 586
ap name lan 587
ap name led 588
ap name link-encryption 588
ap name link-latency 589
ap name location 590
ap name mgmtuser 591
ap name mode 592
ap name monitor-mode 594
ap name monitor-mode dot11b 595
ap name name 596
ap name no dot11 shutdown 596
ap name power 597
ap name shutdown 598
ap name slot shutdown 599
ap name sniff 600
ap name ssh 601
ap name telnet 602
ap name power injector 603
ap name power pre-standard 604
ap name reset-button 604
ap name reset 605
ap name slot 606
ap name static-ip 607
ap name stats-timer 609
ap name syslog host 609
ap name syslog level 610
ap name tcp-adjust-mss 611
ap name tftp-downgrade 612
ap power injector 613
ap power pre-standard 614
ap reporting-period 615
ap reset-button 615
service-policy type control subscriber 616

ap static-ip 617
ap syslog 618
ap name no controller 619
ap tcp-adjust-mss size 620
ap tftp-downgrade 621
config wireless wps rogue client mse 622
clear ap name tsm dot11 all 623
clear ap config 624
clear ap eventlog-all 625
clear ap join statistics 625
clear ap mac-address 626
clear ap name wlan statistics 627
debug ap mac-address 628
show ap cac voice 628
show ap capwap 630
show ap cdp 631
show ap config dot11 632
show ap config dot11 dual-band summary 633
show ap config fnf 633
show ap config 634
show ap crash-file 635
show ap data-plane 635
show ap dot11 l2roam 636
show ap dot11 cleanair air-quality 637
show ap dot11 cleanair config 638
show ap dot11 cleanair summary 640
show ap dot11 640
show ap env summary 645
show ap ethernet statistics 646
show ap gps-location summary 646
show ap groups 647
show ap groups extended 648
show ap image 648
show ap is-supported 649
show ap join stats summary 650

show ap link-encryption 650
show ap mac-address 651
show ap monitor-mode summary 653
show ap name auto-rf 653
show ap name bhmode 655
show ap name bhrate 656
show ap name cac voice 657
show ap name config fnf 658
show ap name dot11 call-control 658
show ap name cable-modem 659
show ap name capwap retransmit 660
show ap name ccx rm 661
show ap name cdp 662
show ap name channel 662
show ap name config 663
show ap name config dot11 665
show ap name config slot 668
show ap name core-dump 671
show ap name data-plane 672
show ap name dot11 673
show ap name dot11 cleanair 676
show ap name env 677
show ap name ethernet statistics 677
show ap name eventlog 678
show ap gps-location summary 679
show ap name image 679
show ap name inventory 680
show ap name lan port 681
show ap name link-encryption 682
show ap name service-policy 683
show ap name tcp-adjust-mss 683
show ap name wlan 684
show ap name wlandot11 service policy 685
show ap slots 686
show ap summary 687

show ap tcp-adjust-mss 688
show ap universal summary 688
show ap uptime 689
show wireless ap summary 690
show wireless client ap 690
test ap name 691
test capwap ap name 692
trapflags ap 693
wireless wps rogue ap rldp alarm-only 694
wireless wps rogue ap rldp auto-contain 695
Mobility 697
MPLS コマンド 699
mobility anchor 699
wireless mobility 701
wireless mobility controller 701
wireless mobility controller (ip_address) 703
wireless mobility controller peer-group 704
wireless mobility group keepalive 705
wireless mobility group member ip 706
wireless mobility group name 707
wireless mobility load-balance 708
show wireless mobility 709
clear wireless mobility statistics 710
マルチプロトコル ラベル スイッチング（MPLS） 713
MPLS コマンド 715
mpls ip default-route 715
mpls ip（グローバル コンフィギュレーション） 716
mpls ip（インターフェイス コンフィギュレーション） 718
mpls label protocol（グローバル コンフィギュレーション） 719
mpls label protocol（インターフェイス コンフィギュレーション） 720
mpls label range 721
show mpls label range 723
マルチキャスト VPN（MVPN） 725
マルチキャスト VPN 727
ip multicast-routing 727

ip multicast mrinfo-filter 729
mdt data 730
mdt default 732
mdt log-reuse 733
show ip pim mdt bgp 734
show ip pim mdt history 736
show ip pim mdt receive 737
show ip pim mdt send 739
Network Management 743
ネットワーク管理コマンド 745
description（ERSPAN） 747
destination（ERSPAN） 748
erspan-id 750
filter（ERSPAN） 751
ip ttl（ERSPAN） 752
ip wccp 753
monitor capture (interface/control plane) 756
monitor capture buffer 760
monitor capture clear 761
monitor capture export 762
monitor capture file 763
monitor capture limit 765
monitor capture match 766
monitor capture start 767
monitor capture stop 768
monitor session 769
monitor session destination 770
monitor session filter 775
monitor session source 777
monitor session type erspan-source 780
origin 781
show ip sla statistics 783
show capability feature monitor 784
show monitor 785
show monitor capture 788

show monitor session 789
show platform ip wccp 791
show platform software swspan 792
snmp-server enable traps 794
snmp-server enable traps bridge 798
snmp-server enable traps bulkstat 799
snmp-server enable traps call-home 800
snmp-server enable traps cef 801
snmp-server enable traps cpu 802
snmp-server enable traps envmon 803
snmp-server enable traps errdisable 804
snmp-server enable traps flash 805
snmp-server enable traps isis 806
snmp-server enable traps license 807
snmp-server enable traps mac-notification 808
snmp-server enable traps ospf 809
snmp-server enable traps pim 811
snmp-server enable traps port-security 812
snmp-server enable traps power-ethernet 813
snmp-server enable traps snmp 814
snmp-server enable traps stackwise 815
snmp-server enable traps storm-control 818
snmp-server enable traps stpx 819
snmp-server enable traps transceiver 820
snmp-server enable traps vrfmib 821
snmp-server enable traps vstack 822
snmp-server engineID 823
snmp-server host 824
source（ERSPAN） 828
switchport mode access 830
switchport voice vlan 830

QoS 833

QoS コマンド 835

auto qos classify 836
auto qos trust 842

auto qos video 849
auto qos voip 859
debug auto qos 872
show auto qos 873
class 874
class-map 877
match（クラスマップ コンフィギュレーション） 879
match non-client-nrt 882
match wlan user-priority 883
policy-map 883
priority 886
queue-buffers ratio 888
queue-limit 890
service-policy（有線） 891
service-policy（WLAN） 893
セット 894
show ap name service-policy 902
show ap name dot11 903
show class-map 905
show platform hardware fed switch 906
show platform software fed switch qos 910
show platform software fed switch qos qsb 912
show wireless client calls 914
show wireless client dot11 915
show wireless client mac-address（コール制御） 916
show wireless client mac-address（TCLAS） 917
show wireless client voice diagnostics 918
show policy-map 919
show wlan 921
trust device 923
Radio Resource Management 925
無線リソース管理コマンド 927
airtime-fairness dot11 mode（apgroup） 929
airtime-fairness dot11 optimization（apgroup） 930
airtime-fairness dot11 policy 931

airtime-fairness policy（wlan） 932
ap dot11 rf-profile 933
ap dot11 rrm 934
ap dot11 rrm ccx 936
ap dot11 rrm channel 937
ap dot11 24ghz rrm channel cleanair-event rogue-contribution 938
ap dot11 24ghz または 5ghz rrm channel dca add 939
ap dot11 24ghz または 5ghz rrm channel dca remove 940
ap dot11 5ghz rrm channel dca chan-width-11n 941
ap dot11 rrm coverage 942
ap dot11 rrm group-member 943
ap dot11 rrm monitor 944
ap dot11 rrm profile 945
ap dot11 rrm tpc-threshold 946
ap dot11 rrm txpower 947
ap dot11 airtime-fairness mode 948
ap dot11 airtime-fairness policy-name 949
policy-weight 950
ap group 950
ap name dot11 airtime-fairness mode 951
ap name dot11 airtime-fairness optimization 952
ap name no dot11 airtime-fairness wlan-name policy-name 953
ap name dot11 airtime-fairness wlan-name policy 954
band-select client 955
band-select cycle 955
band-select expire 956
band-select probe-response 957
channel 958
channel foreign 959
チャネル幅 960
coverage 960
coverage exception 961
coverage level 962
clear wireless airtime-fairness statistics 963
dot11n-only 963

load-balancing 964
high-density clients count 965
high-density clients wlan 966
high-density multicast data-rate 967
high-density rx-sop threshold 968
rate 969
rate mcs 970
trap threshold 970
tx-power 971
tx-power v1 threshold 972
no ap dot11 airtime-fairness policy-name 973
remote-lan 974
rf-profile dot11 24ghz 974
rf-profile dot11 5ghz 975
show ap airtime-fairness ap-group 976
show ap airtime-fairness (ap) 977
show ap airtime-fairness（無線別） 977
show ap airtime-fairness policy（すべて） 978
show ap airtime-fairness wlan 979
show ap dot11 24ghz 979
show ap dot11 5ghz 981
show ap dot11 airtime-fairness（無線帯域） 982
show ap dot11 24ghz rf-profile summary 983
show ap dot11 5ghz rf-profile summary 984
show ap name dot11 airtime-fairness summary 985
show ap name dot11 airtime-fairness policy statistics 985
show ap name dot11 airtime-fairness wlan name statistics 986
show ap rf-profile summary 987
show ap rf-profile name 988
show wireless mobility controller ap 990
シャットダウン 990
wlan 991

Routing 993

双方向フォワーディング検出コマンド 995

authentication（BFD） 995

bfd 996
bfd all-interfaces 998
bfd check-ctrl-plane-failure 999
bfd echo 1000
bfd slow-timers 1002
bfd template 1003
bfd-template 1004
ip route static bfd 1005
ipv6 route static bfd 1007
セキュリティ 1009
セキュリティ コマンド 1011
aaa accounting dot1x 1014
aaa accounting identity 1016
aaa authentication dot1x 1018
aaa authorization 1019
aaa new-model 1024
access-session mac-move deny 1026
action 1027
authentication host-mode 1029
authentication mac-move permit 1030
認証優先 1032
authentication violation 1035
cisp enable 1036
clear errdisable interface vlan 1038
clear mac address-table 1039
cts manual 1041
cts role-based enforcement 1042
cts role-based l2-vrf 1044
cts role-based monitor 1046
cts role-based permissions 1047
deny（MAC アクセス リスト コンフィギュレーション） 1049
device-role（IPv6 スヌーピング） 1052
device-role（IPv6 ND 検査） 1053
device-tracking policy 1055
dot1x critical（グローバル コンフィギュレーション） 1056

dot1x max-start 1057
dot1x pae 1058
dot1x supplicant controlled transient 1059
dot1x supplicant force-multicast 1060
dot1x test eapol-capable 1062
dot1x test timeout 1063
dot1x timeout 1064
epm access-control open 1066
ip access-list role-based 1068
ip admission 1069
ip admission name 1070
ip device tracking maximum 1072
ip device tracking probe 1074
ip dhcp snooping database 1075
ip dhcp snooping information option format remote-id 1077
ip dhcp snooping verify no-relay-agent-address 1078
ip http access-class 1079
ip source binding 1081
ip verify source 1082
ipv6 access-list 1084
ipv6 snooping policy 1086
key chain macsec 1087
limit address-count 1089
mab request format attribute 32 1090
macsec network-link 1092
match（アクセス マップ コンフィギュレーション） 1092
mka pre-shared-key 1094
no authentication logging verbose 1095
no dot1x logging verbose 1096
no mab logging verbose 1097
permit（MAC アクセス リスト コンフィギュレーション） 1098
propagate sgt (cts manual) 1102
protocol（IPv6 スヌーピング） 1104
sap mode-list (cts manual) 1105
security level（IPv6 スヌーピング） 1107

security passthru 1108
show aaa clients 1109
show aaa command handler 1109
show aaa local 1110
show aaa servers 1111
show aaa sessions 1112
show authentication history 1113
show authentication sessions 1114
show cts interface 1116
show cts role-based permissions 1119
show cisp 1121
show dot1x 1122
show eap pac peer 1124
show ip dhcp snooping statistics 1124
show radius server-group 1127
show storm-control 1129
show vlan access-map 1131
show vlan filter 1132
show vlan group 1133
storm-control 1134
switchport port-security aging 1137
switchport port-security mac-address 1139
switchport port-security maximum 1142
switchport port-security violation 1144
tracking（IPv6 スヌーピング） 1146
trusted-port 1148
wireless dot11-padding 1149
wireless security dot1x 1150
wireless security lsc 1152
wireless security strong-password 1153
wireless wps ap-authentication 1154
wireless wps auto-immune 1155
wireless wps cids-sensor 1156
wireless wps client-exclusion 1157
wireless wps mfp infrastructure 1158

wireless wps rogue 1159
wireless wps shun-list re-sync 1160
vlan access-map 1161
vlan filter 1163
vlan group 1164
スタック マネージャおよびハイ アベイラビリティ 1167
スタック マネージャおよびハイ アベイラビリティ コマンド 1169
debug platform stack-manager 1170
main-cpu 1171
mode sso 1172
policy config-sync prc reload 1173
redundancy 1174
redundancy config-sync mismatched-commands 1175
redundancy force-switchover 1177
redundancy reload 1178
reload 1179
session 1180
set trace capwap ap ha 1181
set trace mobility ha 1183
set trace qos ap ha 1185
show checkpoint 1186
show etherchannel summary 1191
show platform ses 1192
show platform stack-manager 1197
show redundancy 1198
show redundancy config-sync 1202
show switch 1204
show trace messages capwap ap ha 1209
show trace messages mobility ha 1210
stack-mac persistent timer 1211
stack-mac update force 1212
standby console enable 1213
switch stack port 1214
switch priority 1216
switch provision 1217

switch renumber 1219

StackWise Virtual コマンド 1221

stackwise-virtual 1221

domain id 1222

stackwise-virtual link 1223

stackwise-virtual dual-active-detection 1224

show stackwise-virtual 1225

システム管理 1229

システム管理コマンド 1231

ap hyperlocation 1234

ap name hyperlocation 1235

hyperlocation 1236

ap ntp ip 1237

ntp ip 1238

arp 1239

boot 1240

cat 1241

clear location 1242

clear location statistics 1243

clear nmsp statistics 1244

clear wireless ccx statistics 1244

clear wireless client tsm dot11 1245

clear wireless location s69 statistics 1246

copy 1247

config-ble 1248

copy startup-config tftp: 1249

copy tftp: startup-config 1250

debug call-admission wireless all 1251

debug rfid 1252

debug voice diagnostics mac-address 1253

debug wps mfp 1253

delete 1254

dir 1255

emergency-install 1257

exit 1259

flash_init 1260
help 1260
license right-to-use 1261
location 1263
location algorithm 1267
location expiry 1268
location notify-threshold 1269
location plm calibrating 1270
location rfid 1271
location rssi-half-life 1272
mac address-table move update 1273
mgmt_init 1274
mkdir 1275
more 1276
nmsp notification interval 1277
no debug all 1278
rename 1279
reset 1280
rmdir 1281
sdm prefer 1282
セット 1283
show avc client 1286
show avc wlan 1287
show cable-diagnostics tdr 1288
show ap hyperlocation 1291
show ap name hyperlocation 1292
show ap group ap-group-name hyperlocation 1293
show debug 1294
show env 1295
show env xps 1297
show flow monitor 1301
show license right-to-use 1306
show location 1308
show location ap-detect 1309
show mac address-table move update 1310

show nmsp 1311
show platform integrity 1312
show platform sudi certificate 1313
show sdm prefer 1315
show tech-support wireless 1316
show wireless band-select 1318
show wireless client calls 1319
show wireless client dot11 1320
show wireless client location-calibration 1321
show wireless client probing 1321
show wireless client summary 1322
show wireless client timers 1323
show wireless client voice diagnostics 1323
show wireless country 1324
show wireless detail 1327
show wireless dtls connections 1328
show wireless flow-control 1329
show wireless flow-control statistics 1330
show wireless load-balancing 1331
show wireless performance 1331
show wireless pmk-cache 1332
show wireless probe 1333
show wireless sip preferred-call-no 1334
show wireless summary 1335
shutdown 1336
system env temperature threshold yellow 1336
test cable-diagnostics tdr 1338
traceroute mac 1339
traceroute mac ip 1342
trapflags 1344
trapflags client 1345
type 1346
unset 1347
version 1349
wireless client 1349

wireless client mac-address deauthenticate 1351
wireless client mac-address 1352
wireless load-balancing 1357
wireless sip preferred-call-no 1358
自律型ネットワーキング コマンド 1361
autonomic adjacency-discovery 1361
autonomic connect 1362
clear autonomic 1363
debug autonomic 1365
show autonomic control-plane 1366
show autonomic device 1367
show autonomic interfaces 1368
show autonomic intent 1369
show autonomic l2-channels 1370
show autonomic service 1371
show autonomic neighbor 1372
トレース コマンド 1375
トレースについて 1375
トレースの概要 1375
トレースログの場所 1376
トレースログの命名規則 1376
ローテーションおよびスロットリング ポリシー 1376
トレース レベル 1377
set platform software trace 1378
show platform software trace filter-binary 1382
show platform software trace message 1383
show platform software trace level 1387
request platform software trace archive 1390
request platform software trace rotate all 1391
request platform software trace filter-binary 1392
set platform software trace wireless switch active R0 hyperlocation 1393
VideoStream 1395
VideoStream コマンド 1397
ap dot11 media-stream multicast-direct 1397
show ap dot11 1398

show wireless media-stream group 1399
wireless media-stream multicast-direct 1400
wireless media-stream 1401
VLAN 1405
VLAN コマンド 1407
client vlan 1408
clear vtp counters 1409
debug platform vlan 1409
debug sw-vlan 1410
debug sw-vlan ifs 1412
debug sw-vlan notification 1413
debug sw-vlan vtp 1415
interface vlan 1416
show platform vlan 1418
show vlan 1419
show vtp 1422
show wireless vlan group 1429
switchport priority extend 1430
switchport trunk 1431
vlan 1434
vlan dot1q tag native 1441
vtp（グローバル コンフィギュレーション） 1442
vtp（インターフェイス コンフィギュレーション） 1448
vtp primary 1449
wireless broadcast vlan 1450
WLAN 1453
WLAN コマンド 1455
aaa-override 1457
accounting-list 1458
assisted-roaming 1459
ap name ap-name lan port-id port-id poe 1460
ap name ap-name lan override 1461
band-select 1462
broadcast-ssid 1463
call-snoop 1464

channel-scan defer-priority 1465
channel-scan defer-time 1466
chd 1467
client association limit 1468
client vlan 1470
ccx aironet-iesupport 1471
datalink flow monitor 1472
device-classification 1473
default 1474
dtim dot11 1477
exclusionlist 1478
exit 1479
exit（WLAN AP グループ） 1479
ip access-group 1480
ip flow monitor 1481
ip verify source mac-check 1482
load-balance 1483
mobility anchor 1484
nac 1486
passive-client 1487
peer-blocking 1488
port 1489
poe 1490
radio 1490
radio-policy 1492
remote-lan 1493
remote-lan 1494
roamed-voice-client re-anchor 1494
security ft 1495
security pmf 1497
security web-auth 1498
security wpa akm 1499
service-policy（WLAN） 1501
session-timeout 1502
show remote-lan all 1503

show remote-lan id 1504
show remote-lan name 1505
show remote-lan summary 1506
show running-config remote-lan 1507
show wlan 1507
show wireless wlan summary 1510
shutdown 1511
sip-cac 1512
static-ip tunneling 1513
vlan 1514
universal-admin 1515
wgb non-cisco 1515
wifidirect policy 1516
wlan（AP グループの設定） 1517
wlan 1518
wlan shutdown 1519
wmm 1520

はじめに

- 表記法，xxxv ページ
- 関連資料，xxxvii ページ
- マニュアルの入手方法およびテクニカル サポート，xxxvii ページ

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、および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。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
`courier` フォントの太字	
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。

表記法	説明
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

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。

ワンポイント アドバイス　時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「translated safety warnings」を参照してください。ステートメント 1071

これらの注意事項を保管しておいてください。

関連資料

（注）　デバイスをインストールまたはアップグレードする前に、デバイスのリリース ノートを参照してください。

- 次の URL にある Cisco Catalyst 3850 スイッチのマニュアル：

  Http://www.cisco.com/go/cat3850_docs

- 次の URL にある Cisco SFP、SFP+、および QSFP+ モジュールのマニュアル（互換性マトリクスを含む）：

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html [英語]

- 次の URL にある Cisco Validated Design（CVD）のマニュアル：

  http://www.cisco.com/go/designzone

- 次の URL にあるエラー メッセージ デコーダ：

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定するこ

ともできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

コマンドライン インターフェイスの使用

この章は、次の内容で構成されています。

- コマンドライン インターフェイスの使用，1 ページ

コマンドライン インターフェイスの使用

この章では、Cisco IOS コマンドライン インターフェイス（CLI）について説明し、CLI を使用してスイッチを設定する方法について説明します。

コマンド モードについて

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。使用可能なコマンドは、現在のモードによって異なります。各コマンド モードで使用できるコマンドのリストを取得するには、システム プロンプトで疑問符（?）を入力します。

スイッチとのセッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーション ステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。スイッチの再起動時には、ユーザ EXEC コマンドは保存されません。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバル コンフィギュレーション モードを開始することもできます。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。コンフィギュレーションを保存するとこれらのコマンドは保存され、スイッチの再起動時に使用されます。各種のコンフィギュレーション モードにアクセスするには、まずグローバル 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。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードを開始できます。

次の表に、主要なコマンド 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。表の例では、ホスト名として*Switch*を使用しています。

表 *1*：コマンド モードの概要

モード	アクセス方式	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとのセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Device#`	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Device(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードを使用して、スイッチ全体に適用されるパラメータを設定します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Device(config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	

モード	アクセス方式	プロンプト	終了方法	モードの用途
				このモードを使用して、VLAN（仮想LAN）パラメータを設定します。VTPモードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が1006以上）を作成してスイッチのスタートアップ コンフィギュレーション ファイルに設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	`Device(config-if)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権EXECモードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、イーサネット ポートのパラメータを設定します。
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 モードで、**line vty** または **line console** コマンドを使用して回線を指定します。	`Device(config-line)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権EXECモードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、端末回線のパラメータを設定します。

コマンド モードの詳細については、このリリースに対応するコマンド リファレンス ガイドを参照してください。

ヘルプ システムについて

システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

表 *2*：ヘルプの概要

コマンド	目的
help	コマンド モードのヘルプ システムの簡単な説明を表示します。

コマンドの先頭部分**?**
 	
`Device# di?`
`dir disable disconnect`
	特定のストリングで始まるコマンドのリストを表示します。

abbreviated-command-entry <Tab>
 	
`Device# sh conf<tab>`
`Device# show configuration`
	特定のコマンド名を補完します。

? `Switch> ?`	特定のコマンドモードで使用可能なすべてのコマンドをリストします。
*command***?** `Switch> show ?`	コマンドに関連するキーワードを一覧表示します。

*command keyword***?**
 	
`Device(config)# cdp holdtime ?`
`  <10-255> Length of time (in sec) that receiver must keep this packet`
	キーワードに関連する引数を一覧表示します。

コマンドの省略形

コマンドの先頭から、スイッチが特定のコマンドとして認識できる文字数だけを入力し、後は省略できます。

show configuration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
Device# show conf
```

コマンドの no 形式および default 形式の概要

大部分のコンフィギュレーション コマンドに、**no** 形式があります。**no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**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と、インターフェイスのシャットダウンが取り消されます。ディセーブルにした機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにするには、キーワード **no** を指定せずにコマンドを使用します。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージについて

次の表に、CLI を使用してスイッチを設定するときに表示される可能性のあるエラー メッセージの一部を紹介します。

表 *3* : *CLI* の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	スイッチがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。間違っている箇所をキャレット（^）記号で示しています。	疑問符（?）を入力すると、そのコマンド モードで使用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギングの使用方法

スイッチの設定変更を記録して表示させることができます。Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザ ベースごとに変更内容をトラッキングできます。ログに記録されるのは、適用された各コンフィギュレーション コマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターン コードです。この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。Syslog へこの通知を送信することも選択できます。

（注） CLI または HTTP の変更のみがログとして記録されます。

コマンド履歴の使用

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、10 のコマンドラインが履歴バッファに保存されます。現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。これらの手順は任意です。

現在の端末セッションで保存されるコマンドライン数を変更するには、特権 EXEC モードで次のコマンドを入力します。

```
Device# terminal history [size number-of-lines]
```

指定できる範囲は 0 ～ 256 です。

特定の回線に関するすべてのセッションで保存されるコマンドライン数を設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
Device(config-line)# history [size number-of-lines]
```

指定できる範囲は 0 ～ 256 です。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。これらの操作は任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 *4*：コマンドの呼び出し

アクション	結果
Ctrl+P キーまたは↑キーを押します。	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。

アクション	結果
Ctrl+N キーまたは↓キーを押します。	**Ctrl+P** または上矢印キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
show history `Device(config)# help`	特権EXECモードで、直前に入力したいくつかのコマンドを一覧表示します。表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定値によって制御されます。

コマンド履歴機能の無効化

コマンド履歴機能は、自動的にイネーブルになっています。現在の端末セッションまたはコマンドラインでディセーブルにできます。これらの手順は任意です。

現在の端末セッションでこの機能をディセーブルにするには、**terminal no history** 特権 EXEC コマンドを使用します。

回線に関するセッションでコマンド履歴をディセーブルにするには、**no history** ライン コンフィギュレーション コマンドを使用します。

編集機能の使用方法

ここでは、コマンドラインの操作に役立つ編集機能について説明します。

編集機能の有効化および無効化

拡張編集モードは自動的にイネーブルになりますが、ディセーブルにする、再びイネーブルにする、または特定の回線で拡張編集機能を使用できるように設定できます。これらの手順は任意です。

拡張編集モードをグローバルにディセーブルにするには、ラインコンフィギュレーションモードで次のコマンドを入力します。

```
Switch (config-line)# no editing
```

現在の端末セッションで拡張編集モードを再びイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Device# terminal editing
```

特定の回線について拡張編集モードを再び設定するには、ラインコンフィギュレーションモードで次のコマンドを入力します。

```
Device(config-line)# editing
```

キーストロークによるコマンドの編集

このテーブルに、コマンドラインの編集に必要なキーストロークを示します。これらのキーストロークは任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 *5*：キーストロークによるコマンドの編集

機能	キーストローク	目的
コマンドライン上を移動して、変更または訂正を行います。	**Ctrl+B** または左矢印キーを押します。	カーソルを 1 文字後退させます。
	Ctrl+F または右矢印キーを押します。	カーソルを 1 文字前進させます。
	Ctrl+A を押します。	コマンドラインの先頭にカーソルを移動します。
	Ctrl+E を押します。	カーソルをコマンド ラインの末尾に移動します。
	Esc+B を押します。	カーソルを 1 単語後退させます。
	Esc+F を押します。	カーソルを 1 単語前進させます。
	Ctrl+T を押します。	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
バッファからコマンドを呼び出し、コマンドラインにペーストします。最後に削除した 10 項目がバッファに保存されています。	Ctrl+Y を押します。	バッファ内の最新のエントリを呼び出します。

機能	キーストローク	目的
	Esc+Y を押します。	次のバッファ エントリを呼び出します。 バッファには、最後に削除またはカットした 10 項目しか保存されません。Esc+Y を 11 回以上押すと、最初のバッファ エントリに戻って表示されます。
不要なエントリを削除します。	Delete キーまたは Backspace キーを押します。	カーソルの左にある文字を消去します。
	Ctrl+D を押します。	カーソル位置にある文字を削除します。
	Ctrl+K を押します。	カーソル位置からコマンド ラインの末尾までのすべての文字を削除します。
	Ctrl+U または Ctrl+X を押します。	カーソル位置からコマンド ラインの先頭までのすべての文字を削除します。
	Ctrl+W を押します。	カーソルの左にある単語を削除します。
	Esc+D を押します。	カーソルの位置から単語の末尾までを削除します。
ワードを大文字または小文字にします。または、一連の文字をすべて大文字にします。	Esc+C を押します。	カーソル位置のワードを大文字にします。
	Esc+L を押します。	カーソルの場所にある単語を小文字にします。
	Esc+U を押します。	カーソルの位置から単語の末尾までを大文字にします。
特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。	Ctrl+V または Esc+Q キーを押します。	

機能	キーストローク	目的
1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注） **show** コマンドの出力など、端末画面に一度に表示できない長い出力では、More プロンプトが使用されます。More プロンプトが表示された場合は、Return キーおよびSpace キーを使用してスクロールできます。	Return キーを押します。	1 行下にスクロールします。
	Space キーを押します。	1 画面分下にスクロールします。
スイッチから画面にメッセージが突然送られた場合に、現在のコマンド ラインを再表示します。	Ctrl+L または Ctrl+R を押します。	現在のコマンド ラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で 1 行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは10文字分だけ左へシフトされます。コマンドラインの先頭から10文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、Ctrl+B キーまたは←キーを繰り返し押します。コマンドラインの先頭に直接移動するには、Ctrl+A を押します。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次の例では、**access-list** グローバル コンフィギュレーション コマンド エントリが 1 行分よりも長くなっています。最初にカーソルが行末に達すると、その行は10文字分だけ左へシフトされ、再表示されます。ドル記号（$）は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び 10 文字分だけ左へシフトされます。

```
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Device(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
```

```
Device(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Device(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

コマンドの入力が終わった後、Ctrl+A を押して全体の構文をチェックし、その後 Return キーを押してコマンドを実行してください。行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。

```
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

ソフトウェアでは、端末画面は80カラム幅であると想定されています。それ以外の幅の場合は、特権 EXEC コマンド **terminal width** を使用してターミナルの幅を設定します。

ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。これらのコマンドの使用は任意です。

この機能を使用するには、**show** または **more** コマンドを入力した後、パイプ記号（|）、**begin**、**include**、または **exclude** のいずれかのキーワード、および文字列（検索またはフィルタの条件）を指定します。

command | {**begin** | **include** | **exclude**} *regular-expression*

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

次の例では、*protocol* が使用されている行だけを出力するように指定する方法を示します。

```
Device# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```

CLI のアクセス

CLI にはコンソール接続、Telnet、またはブラウザを使用することによってアクセスできます。

スイッチ スタックおよびスタック メンバ インターフェイスは、アクティブ スイッチを経由して管理します。スイッチごとにスタック メンバを管理することはできません。1 つまたは複数のスタック メンバーのコンソール ポートまたはイーサネット管理ポートを経由してアクティブ スイッチへ接続できます。複数の CLI セッションをアクティブ スイッチに使用する場合は注意が必要です。1つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。

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

特定のスタック メンバ ポートを設定する場合は、CLI コマンド インターフェイス表記にスタック メンバ番号を含めてください。

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

コンソール接続または Telnet による CLI アクセス

CLI にアクセスするには、スイッチのハードウェア インストレーション ガイドに記載されている手順で、スイッチのコンソール ポートに端末または PC を接続するか、または PC をイーサネット管理ポートに接続して、スイッチの電源をオンにする必要があります。

CLI アクセスはスイッチのセットアップの前に使用できます。スイッチが設定された後は、リモート Telnet セッションまたは SSH クライアントで CLI にアクセスできます。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチのコンソール ポートに管理ステーションまたはダイヤルアップ モデムを接続するか、イーサネット管理ポートに PC を接続します。コンソール ポートまたはイーサネット管理ポートへの接続については、スイッチのハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化セキュア シェル（SSH）パッケージを使用します。スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブル シークレット パスワードを設定しておくことも必要です。

  スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

  スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソール ポート、イーサネット管理ポート、Telnet セッション、または SSH セッションを通じて接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。

第 I 部

キャンパス ファブリック コマンド

- キャンパス ファブリック コマンド，17 ページ

第 2 章

キャンパス ファブリック コマンド

-
- border, 17 ページ
- コンテキスト, 18 ページ
- control-plane, 19 ページ
- domain, 20 ページ
- debug fabric auto, 21 ページ
- fabric auto, 22 ページ
- host-pool name, 23 ページ
- show fabric domain, 24 ページ
- show fabric context, 25 ページ
- show fabric host-pool, 26 ページ

border

border *ip address*

構文の説明

ip address	ファブリック境界デバイスの IP アドレスを設定します。

コマンド デフォルト

なし。

コマンド モード

ファブリック自動ドメイン構成

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ファブリック境界デバイスの IP アドレスを設定するには、このコマンドを使用します。ファブリック ドメインの境界デバイスは、従来のレイヤ 3 ネットワークまたは異なるファブリック ドメインをローカル ドメインに接続し、到達可能性とポリシー（VRF および SGT）に関する情報を 1 つのドメインから別のドメインに変換します。ファブリック境界デバイスは、LISP のプロキシ出力トンネル ルータに対応します。

このコマンドは、LISP 設定を自動生成し、ファブリック オーバーレイを編成します。**show-running configuration** コマンドは、自動生成されたコマンドを含むファブリック ドメインの設定を表示します。

例

次の設定は、このコマンドがデバイスで動作している場合に自動生成されます。

```
Device(config-fabric-auto-domain)#border 198.51.100.4

    ipv4 use-petr 198.51.100.4 priority 10 weight 10
```

ipv4 proxy etr コマンドの詳細については、『LISP Command Reference（LISP コマンド リファレンス）』を参照してください。

コンテキスト

context name *name* **id** *id*

構文の説明

context name	ファブリック ドメインで新しいレイヤ 3 コンテキストを作成します。
id*id*	コンテキストに ID を割り当てます。

コマンド デフォルト

なし

コマンド モード

ファブリック自動ドメイン構成モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

仮想コンテキストは、レイヤ 3 ルーティング テーブルの複数のインスタンスを作成するために、Virtual Routing and Forwarding（VRF）を使用して、デバイス レベルで仮想化を提供します。コンテキストまたはVRFは、IPアドレス全体のセグメンテーションを行い、オーバーラップしたアドレス空間とトラフィックの分離を可能にします。\

このコマンドは、LISP（ロケータ ID 分離プロトコル）とVRF（Virtual Routing and Forwarding）設定の自動生成を有効にして、ファブリック オーバーレイを編成します。**show-running configuration** コマンドは、自動生成されたベース ライン コマンドを含む仮想コンテキストの設定を表示します。

例

```
Device(config-fabric-auto-domain)#context name guest
id 10
```

次の設定は、このコマンドがデバイスで動作している場合に自動生成されます。

```
ip vrf  guest
    description Auto-provisioned vrf  for context example-context (source - fabric auto)
router lisp
     eid-table vrf  guest instance-id 10
```

control-plane

control-plane {*ip address*|**auth-key***key*}

構文の説明

ip address	コントロール プレーン デバイスのIPアドレスを設定します。
auth-key*key*	コントロール プレーン デバイスへのアクセスを認証するキーを設定します。

コマンド デフォルト

なし

コマンド モード

ファブリック自動ドメイン構成モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ファブリック エッジ デバイスがコントロール プレーン デバイスと通信できるようにするには、このコマンドを使用してコントロール プレーン デバイスの IP アドレスおよび認証キーを設定します。

このコマンドは、LISP設定を自動生成し、ファブリック オーバーレイを編成します。**show-running configuration** コマンドは、自動生成されたコマンドを含むファブリック ドメインの設定を表示します。

例

次の設定は、このコマンドがデバイスで動作している場合に自動生成されます。

```
Device(config-fabric-auto-domain)#control-plane 2.2.2.2
auth_key examplekey123
router lisp
locator-set default.RLOC
ipv4-interface Loopback0 priority 10 weight 10
exit

disable-ttl-propagate
ipv4 sgt
eid-table default instance-id 0
exit

loc-reach-algorithm lsb-reports ignore
ipv4 itr map-resolver 2.2.2.2
ipv4 itr
ipv4 etr map-server 2.2.2.2 key examplekey123
ipv4 etr
```

ipv4 map-server and **ipv4 map-resolver** コマンドの詳細については、『LISP Command Reference（LISP コマンド リファレンス）』を参照してください。

domain

ファブリック ドメインを設定し、ファブリック自動ドメイン コンフィギュレーション モードを開始します。このコマンドの **no** バージョンを使用すると、ファブリック ドメインが削除されます。

domain { **default**| **name** *name*}

no domain

構文の説明

default	デフォルトのファブリック ドメインを設定し、ファブリック自動ドメイン コンフィギュレーション モードを開始します。
name *name*	新しいファブリック ドメインを設定し、ファブリック自動ドメイン コンフィギュレーション モードを開始します。

コマンド デフォルト

なし

コマンド モード

ファブリック自動コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ネットワークが新しいドメインを作成するように要求しない限り、デフォルト ドメインを使用することを推奨します。このコマンドは、ファブリック ドメインでのエッジ、コントロールプレーンおよび境界デバイスの設定を可能にする、ファブリック自動ドメイン コンフィギュレーション モードの開始を許可します。

例

```
Device(config-fabric-auto)#domain default
Device(config-fabric-auto)#domain name exampledomain
```

debug fabric auto

debug fabric auto{**trace**| **level**| {**error**| **verbose**}}

構文の説明

trace	ファブリック自動コマンドが実行されると自動生成されるコマンドのトレースを有効にします。

level error	ファブリック オーバーレイ プロビジョニング時に発生したエラーを表示します。
level verbose	ファブリック オーバーレイ プロビジョニング時に発生したメッセージの最大数を表示します。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ファブリック ドメイン設定のトラブルシューティングを行い、**fabric auto** コマンドによって自動生成されるコマンドをトレースし、発生したエラーを表示するには、これらのデバッグ コマンドを使用します。

no debug fabric auto level verbose コマンドは、ファブリック プロビジョニング時に発生するすべてのメッセージの表示を無効にします。

fabric auto

自動ファブリック プロビジョニングを有効にして自動ファブリック 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 **fabric auto** コマンドを使用します。

fabric auto

構文の説明

fabric auto	自動ファブリック プロビジョニングを有効にして、ファブリック自動コンフィギュレーション モードを開始します。

コマンド デフォルト

なし。グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

fabric auto コマンドは、ファブリック ドメイン内のすべての要素を自動的に設定することを可能にします。またこのコマンドは、自動生成 LISP、VLAN、VRF 設定を有効にして、ファブリック オーバーレイを編成します。**show-running configuration** コマンドは、自動生成されたベース ライン コマンドを含むファブリック ドメインの設定を表示します。

例

```
Device(config)#fabric auto
```

host-pool name

ファブリック ドメインのエンドポイントをグループ化するための IP プールを作成し、ホスト プール コンフィギュレーション モードを開始します。

host-poolname*name*{ **vlan** *ID*| **gateway***ipv4 -address/subnet mask* | **context name***name*| **use-dhcp***ip4 address*}

構文の説明

vlan*ID*	ホスト プールに関連付ける VLAN ID を設定します。
context name*name*	コンテキストまたは VRF をホスト プールに関連付けます。
gateway*ipv4 address/subnet mask*	ホスト プールのルーティング ゲートウェイ IP アドレスとサブネット マスクを設定します。
use-dhcp*ipv4 address*	ホスト プールの DHCP サーバを設定します。

コマンド デフォルト

なし

コマンド モード

ファブリック自動ドメイン構成モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

host-pool コマンドを使用して、ファブリック ドメイン内のエンドポイントを IP プールにグループ化し、VLAN ID および IP サブネットで識別します。

このコマンドは、LISP 設定を自動生成し、ファブリック オーバーレイを編成します。**show-running configuration** コマンドは、自動生成されたコマンドを含むファブリック ドメインの設定を表示します。

例

この例では、ファブリック ドメインのホスト プールを設定します。

```
device(config-fabric-auto-domain)#host-pool name VOICE_DOMAIN
device(config-fabric-auto-domain-host-pool)#vlan 10
device(config-fabric-auto-domain-host-pool)#context name example-context
device(config-fabric-auto-domain-host-pool)#gateway 192.168.1.254/24
device(config-fabric-auto-domain-host-pool)#use-dhcp 172.10.1.1
device(config-fabric-auto-domain-host-pool)#exit
```

この設定は、ホスト プールを設定するときに自動生成されます。

```
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp snooping vlan 10
ip dhcp snooping
vlan 10
name VOICE_DOMAIN
interface Vlan10
ip vrf forwarding example-context
ip dhcp relay source-interface Loopback0
ip address 192.168.1.254 255.255.255.0
ip helper-address global 209.65.201.6
no ip redirects
ip local-proxy-arp
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility example-context.EID.VOICE_DOMAIN
!
router lisp
eid-table vrf example-context
dynamic-eid example-context.EID.VOICE_DOMAIN
database-mapping 192.168.1.0/24 locator-set default.RLOC
```

show fabric domain

show fabric domain

コマンド モード

特権 EXEC

のドメイン、およびデフォルトのコンテキスト

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ファブリック ドメインの概要を表示するには、このコマンドを使用します。次に、エッジデバイスの出力例を示します。

```
device#show fabric domain
Fabric Domain : "default"
Role : Edge
Control-Plane Service: Disabled
Number of "Control-Plane" node(s): 2
IP Address           Auth-key
---------------------------------
192.168.1.4          example-key1
192.168.1.5          example-key2

Number of "Border" node(s): 1
 IP Address
---------------
 192.168.1.6

Number of context(s): 2
 Codes: * - Not Configured

 Name                ID        Host-pools
-------------------------------------------------
default              0          *
example-context      10         1
```

show fabric context

show fabriccontext[**default**| *name*]

構文の説明

default	デフォルト コンテキスト
name	ファブリック ドメインのコンテキストの名前

コマンド デフォルト

デフォルト コンテキスト

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ファブリック ドメインのコンテキスト設定の概要を表示するには、このコマンドを使用します。

```
device#show fabric context
Fabric-domain: default
Number of context(s): 2
 Name                ID        Host-pools
-----------------------------------------------
default              0          *
example-context      10         1

* - Not Configured
```

show fabric host-pool

show fabrichost-pool*name*

構文の説明

name	ホスト プールの名前

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

指定されたホスト プールの設定を表示するには、このコマンドを使用します。

```
device# show fabric host-pool
Fabric Domain : "default"
 context: default
   Number of host-pools : 0
   name            vlan    prefix               gateway           use-dhcp
 ------------------------------------------------------------------------------

 context: example-context
   Number of host-pools : 1
   name            vlan    prefix               gateway           use-dhcp
 ------------------------------------------------------------------------------
  VOICE_DOMAIN     10      192.168.1.0/24        192.168.1.254     209.65.201.6
```

第 II 部

CleanAir

- CleanAir コマンド，31 ページ

第 3 章

CleanAir コマンド

- ap dot11 5ghz cleanair , 32 ページ
- ap dot11 5ghz cleanair alarm air-quality, 33 ページ
- ap dot11 5ghz cleanair alarm device, 34 ページ
- default ap dot11 5ghz cleanair device, 35 ページ
- ap dot11 5ghz rrm channel cleanair-event, 36 ページ
- ap dot11 5ghz rrm channel device, 38 ページ
- ap dot11 24ghz cleanair, 39 ページ
- ap dot11 24ghz cleanair alarm air-quality, 40 ページ
- ap dot11 24ghz cleanair alarm device, 41 ページ
- default ap dot11 24ghz cleanair device, 42 ページ
- ap dot11 24ghz rrm channel cleanair-event, 45 ページ
- ap dot11 24ghz rrm channel device, 46 ページ
- ap name mode se-connect, 47 ページ
- default ap dot11 5ghz cleanair device, 48 ページ
- default ap dot11 5ghz rrm channel cleanair-event, 49 ページ
- default ap dot11 5ghz rrm channel device, 50 ページ
- default ap dot11 24ghz cleanair alarm device, 51 ページ
- default ap dot11 24ghz cleanair device, 52 ページ
- default ap dot11 24ghz rrm channel cleanair-event, 55 ページ
- show ap dot11 5ghz cleanair air-quality summary, 56 ページ
- show ap dot11 5ghz cleanair air-quality worst, 56 ページ

- show ap dot11 5ghz cleanair config, 57 ページ
- show ap dot11 5ghz cleanair device type, 59 ページ
- show ap dot11 24ghz cleanair air-quality summary, 60 ページ
- show ap dot11 24ghz cleanair air-quality worst, 61 ページ
- show ap dot11 24ghz cleanair config, 61 ページ
- show ap dot11 24ghz cleanair summary, 63 ページ

ap dot11 5ghz cleanair

5 GHz デバイスを検出するために CleanAir を有効にするには、グローバル コンフィギュレーション モードで **apdot115ghzcleanair** コマンドを使用します。

ap dot11 5ghz cleanair

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

他の CleanAir コマンドを設定する前に、この CleanAir コマンドを有効にする必要があります。

次に、5 GHz デバイス用の CleanAir を有効にする例を示します。

```
Device(config)# ap dot11 5ghz cleanair
```

関連トピック

ap dot11 5ghz cleanair alarm air-quality, （33 ページ）

ap dot11 5ghz cleanair alarm device, （34 ページ）

default ap dot11 5ghz cleanair device, （35 ページ）

ap dot11 5ghz rrm channel cleanair-event, （36 ページ）
ap dot11 5ghz rrm channel device, （38 ページ）

ap dot11 5ghz cleanair alarm air-quality

電波品質（AQ）が 5 GHz デバイスのしきい値に達した場合のアラームを設定するには、**apdot115ghzcleanairalarmair-quality** コマンドを使用します。AQ が 5 GHz デバイスのしきい値に達した場合のアラームを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz cleanair alarm air-quality threshold *threshold _value*

構文の説明

threshold *threshold _value*	電波品質のしきい値を設定します。範囲は 1 ～ 100 です。

コマンド デフォルト

AQ のデフォルトのしきい値は 10 です。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 5ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、AQ のしきい値を設定する例を示します。

```
Device(config)# ap dot11 5ghz cleanair alarm air-quality threshold 30
```

関連トピック

ap dot11 5ghz cleanair , （32 ページ）
default ap dot11 5ghz cleanair device, （35 ページ）

ap dot11 5ghz cleanair alarm device

5 GHz 干渉デバイスのアラームを設定するには、**apdot115ghzcleanairalarmdevice** コマンドを使用します。

ap dot11 5ghz cleanair alarm device {**canopy**| **cont-tx**| **dect-like**| **inv**| **jammer**| **nonstd**| **radar**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**}

構文の説明

canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
radar	レーダーのアラームを設定します。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi反転デバイスのアラームが有効になっており、他のすべての干渉デバイスのアラームは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 5ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、レーダー デバイスからの干渉を通知するアラームを有効にする例を示します。

```
Device(config)# ap dot11 5ghz cleanair alarm device radar
```

関連トピック

ap dot11 5ghz cleanair , （32 ページ）

ap dot11 5ghz cleanair alarm air-quality, （33 ページ）

default ap dot11 5ghz cleanair device

5 GHz 干渉デバイスのアラームのデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **defaultapdot115ghzcleanairdevice** コマンドを使用します。

default ap dot11 5ghz cleanair device {**canopy**| **cont-tx**| **dect-like**| **inv**| **jammer**| **nonstd**| **radar**| **report**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**}

構文の説明

canopy	canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）と同様の電話機のアラームを設定します。
inv	スペクトラム反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害装置干渉デバイスのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
radar	レーダーのアラームを設定します。

report	干渉デバイスのレポートを有効にします。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi反転デバイスのアラームは有効になっています。その他の干渉デバイスのアラームはすべて無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 5ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、CleanAir によるビデオ カメラの干渉時のレポートを有効にする例を示します。

```
Device(config)# default ap dot11 5ghz cleanair device video
```

ap dot11 5ghz rrm channel cleanair-event

イベント駆動型 RRM（EDRRM）を有効にして 5 GHz デバイスの感度を設定するには、グローバル コンフィギュレーション モードで **apdot115ghzrrmchannelcleanair-event** コマンドを使用します。EDRRM を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high**| **low**| **medium**}]

no ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high**| **low**| **medium**}]

構文の説明

sensitivity	（任意）CleanAir イベントの EDRRM 感度を設定します。
high	（任意）電波品質（AQ）の値で示される、非 Wi-Fi 干渉に対する最も高い感度を指定します。
low	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する最も低い感度を指定します。
medium	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する中程度の感度を指定します。

コマンド デフォルト

EDRRM が無効になっており、EDRRM 感度は low 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（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

感度を設定する前に、**ap dot11 5ghz rrm channel cleanair-event** コマンドを使用して EDRRM を有効にする必要があります。

次に、EDRRM を有効にして EDRRM 感度を high に設定する例を示します。

```
Device(config)# ap dot11 5ghz rrm channel cleanair-event
Device(config)# ap dot11 5ghz rrm channel cleanair-event sensitivity high
```

関連トピック

ap dot11 5ghz cleanair , （32 ページ）

ap dot11 5ghz rrm channel device, （38 ページ）

ap dot11 5ghz rrm channel device

802.11a チャネルで永続型非 Wi-Fi デバイス回避を設定するには、グローバル コンフィギュレーション モードで **apdot115ghzrrmchanneldevice** コマンドを使用します。永続型デバイス回避を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz rrm channel device

no ap dot11 5ghz rrm channel device

構文の説明

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

CleanAir 永続型デバイス ステートが無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

CleanAir 対応モニタ モード アクセス ポイントは、すべての設定済みチャネル上の永続型デバイスに関する情報を収集し、その情報をデバイスに保存します。ローカル モードおよびブリッジ モードのアクセス ポイントは、稼働チャネルでのみ干渉デバイスを検出します。

次に、802.11a デバイスで永続型デバイス回避を有効にする例を示します。

```
Device(config)# ap dot11 5ghz rrm channel device
```

関連トピック

ap dot11 5ghz cleanair , （32 ページ）

ap dot11 5ghz rrm channel cleanair-event, （36 ページ）

ap dot11 24ghz cleanair

2.4GHzデバイスを検出するためにCleanAirを有効にするには、グローバル コンフィギュレーション モードで **apdot1124ghzcleanair** コマンドを使用します。2.4GHz デバイスを検出するための CleanAir を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz cleanair

構文の説明

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

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

他の CleanAir コマンドを設定する前に、この CleanAir コマンドを有効にする必要があります。

次に、2.4 GHz デバイス用の CleanAir を有効にする例を示します。

```
Device(config)# ap dot11 24ghz cleanair
```

関連トピック

ap dot11 24ghz cleanair alarm air-quality, （40 ページ）

ap dot11 24ghz cleanair alarm device, （41 ページ）

default ap dot11 24ghz cleanair device, （42 ページ）

ap dot11 24ghz rrm channel cleanair-event, （45 ページ）

ap dot11 24ghz rrm channel device, （46 ページ）

ap dot11 24ghz cleanair alarm air-quality

すべての 2.4GHz デバイスの電波品質しきい値に関する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 **apdot1124ghzcleanairalarmair-quality** コマンドを使用します。すべての 2.4GHz デバイスの AQ しきい値に関するアラームを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz cleanair alarm air-quality threshold *threshold_value*

構文の説明

threshold *threshold_value*	AQ のしきい値を設定します。範囲は 1 ～ 100 です。

コマンド デフォルト

AQ のデフォルトのしきい値は 10 です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、AQ のしきい値を設定する例を示します。

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality threshold 50
```

関連トピック

ap dot11 24ghz cleanair, （39 ページ）

ap dot11 24ghz cleanair alarm device, （41 ページ）

default ap dot11 24ghz cleanair device, （42 ページ）

ap dot11 24ghz cleanair alarm device

2.4GHz 干渉デバイスの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 **apdot1124ghzcleanairalarmdevice** コマンドを使用します。2.4GHz 干渉デバイスのアラームを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz cleanairalarm {**device | bt-discovery| bt-linkcanopy| cont-tx| dect-like | fh| inv| jammer | mw-oven| nonstd| superag| tdd-txvideo| wimax-fixed| wimax-mobile| xbox| zigbee**}

構文の説明

bt-discovery	Bluetooth 干渉デバイスのアラームを設定します。
bt-link	Bluetooth リンクのアラームを設定します。
canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
fh	802.11 周波数ホッピング（FH）デバイスのアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
mw-oven	電子レンジのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。
xbox	Xbox 干渉デバイスのアラームを設定します。
zigbee	802.15.4 干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi反転デバイスのアラームが有効になっています。他のすべてのデバイスのアラームは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、ZigBee デバイスからの干渉を通知するアラームを有効にする例を示します。

```
Device(config)# ap dot11 24ghz cleanair alarm device zigbee
```

関連トピック

ap dot11 24ghz cleanair, （39 ページ）

ap dot11 24ghz cleanair alarm air-quality, （40 ページ）

default ap dot11 24ghz cleanair device, （42 ページ）

default ap dot11 24ghz cleanair device

2.4 GHz干渉デバイスのレポート生成のデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **defaultapdot1124ghzcleanairdevice** コマンドを使用します。

default ap dot11 24ghz cleanair device {**ble-beacon**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fh**| **inv**| **jammer**| **mw-oven**| **nonstd**| **report**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**}

構文の説明

ble-beacon	BLE ビーコン機能を設定します。

bt-discovery	Bluetooth 干渉デバイスのアラームを設定します。
bt-link	任意の Bluetooth リンクのアラームを設定します。
canopy	canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）と同様の電話機のアラームを設定します。
fh	802.11 周波数ホッピングデバイスのアラームを設定します。
inv	スペクトラム反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害装置干渉デバイスのアラームを設定します。
mw-oven	電子レンジのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオカメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。

wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。
xbox	Xbox 干渉デバイスのアラームを設定します。
zigbee	802.15.4 干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi反転デバイスのアラームは有効になっています。その他のデバイスのアラームはすべて無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	このコマンドが変更されました。**ble-beacon** キーワードが追加されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、CleanAir によるビデオ カメラの干渉時のレポートを有効にする例を示します。

```
Device(config)# default ap dot11 24ghz cleanair device video
```

関連トピック

ap dot11 24ghz cleanair, （39 ページ）

ap dot11 24ghz cleanair alarm air-quality, （40 ページ）

ap dot11 24ghz cleanair alarm device, （41 ページ）

ap dot11 24ghz rrm channel cleanair-event

イベント駆動型 RRM（EDRRM）を有効にして 2.4 GHz デバイスの感度を設定するには、グローバル コンフィギュレーション モードで **apdot1124ghzrrmchannelcleanair-event** コマンドを使用します。EDRRM を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz rrm channel cleanair-event sensitivity {**high**| **low**| **medium**}

no ap dot11 24ghz rrm channel cleanair-event [**sensitivity**{**high**| **low**| **medium**}]

構文の説明

sensitivity	（任意）CleanAir イベントの EDRRM 感度を設定します。
high	（任意）電波品質（AQ）の値で示される、非 Wi-Fi 干渉に対する最も高い感度を指定します。
low	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する最も低い感度を指定します。
medium	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する中程度の感度を指定します。

コマンド デフォルト

EDRRM が無効になっており、感度は low 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（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

感度を設定する前に、**ap dot11 24ghz rrm channel cleanair-event** コマンドを使用して EDRRM を有効にする必要があります。

次に、EDRRM を有効にして EDRRM 感度を low に設定する例を示します。

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity low
```

関連トピック

ap dot11 24ghz cleanair, （39 ページ）

ap dot11 24ghz rrm channel device, （46 ページ）

ap dot11 24ghz rrm channel device

802.11b チャネルで永続型非 Wi-Fi デバイス回避を設定するには、グローバル コンフィギュレーション モードで **apdot1124ghzrrmchanneldevice** コマンドを使用します。永続型デバイス回避を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz rrm channel device

no ap dot11 24ghz rrm channel device

構文の説明

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

永続型デバイス回避が無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

CleanAir 対応モニタ モードアクセス ポイントは、すべての設定済みチャネル上の永続型デバイスに関する情報を収集し、その情報をデバイスに保存します。ローカル モードおよびブリッジ モードのアクセス ポイントは、稼働チャネルでのみ干渉デバイスを検出します。

次に、永続型デバイス回避を有効にする例を示します。

```
Device(config)# ap dot11 24ghz rrm channel device
```

関連トピック

ap dot11 24ghz cleanair, （39 ページ）

ap dot11 24ghz rrm channel cleanair-event, （45 ページ）

ap name mode se-connect

アクセス ポイントを SE-Connect モードに設定するには、特権 EXEC モードで **ap name***ap_name***mode se-connect** コマンドを使用します。

ap name*ap_name***mode se-connect**

構文の説明

ap_name	アクセス ポイントの名前。

コマンド デフォルト

どのアクセス ポイントも SE-Connect モードに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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

アクセス ポイントは、モードを変更した後に再起動します。

SE-Connect モードを使用すると、外部の Microsoft Windows XP または Vista PC で実行されている Spectrum Expert アプリケーションを Cisco CleanAir 対応のアクセス ポイントに接続して、詳細なスペクトラム データを表示および分析できるようになります。Spectrum Expert アプリケーションは、コントローラをバイパスしてアクセス ポイントに直接接続します。SE-Connect モードのアクセス ポイントからは、Wi-Fi、RF、スペクトラム データがコントローラに提供されません。すべての CleanAir システム機能は、AP がこのモードになっていて、クライアントが実行されていない

間、一時停止状態になります。このモードは、リモート トラブルシューティングのみを対象としています。

次に、アクセス ポイントのモードを SE-Connect に変更する例を示します。

```
Device# ap name AS-5508-5-AP3 mode se-connect

Changing the AP's mode will cause the AP to reboot.
Are you sure you want to continue? (y/n)[y]: y
% switch-1:wcm:Cisco AP does not support the seconnect mode
```

default ap dot11 5ghz cleanair device

5 GHz 干渉デバイスのアラームのデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **defaultapdot115ghzcleanairdevice** コマンドを使用します。

default ap dot11 5ghz cleanair device {**canopy| cont-tx| dect-like| inv| jammer| nonstd| radar| report| superag| tdd-tx| video| wimax-fixed| wimax-mobile**}

構文の説明

canopy	canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）と同様の電話機のアラームを設定します。
inv	スペクトラム反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害装置干渉デバイスのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
radar	レーダーのアラームを設定します。
report	干渉デバイスのレポートを有効にします。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi反転デバイスのアラームは有効になっています。その他の干渉デバイスのアラームはすべて無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 5ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、CleanAir によるビデオ カメラの干渉時のレポートを有効にする例を示します。

```
Device(config)# default ap dot11 5ghz cleanair device video
```

default ap dot11 5ghz rrm channel cleanair-event

5 GHz デバイスのイベント駆動型無線リソース管理（EDRRM）のデフォルトの状態と EDRRM 感度を設定するには、グローバル コンフィギュレーション モードで **default apdot115ghzrrmchannelcleanair-event** コマンドを使用します。

default ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high**| **low**| **medium**}]

構文の説明

sensitivity	（任意）CleanAir イベントの EDRRM 感度を設定します。
high	（任意）電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。
low	（任意）電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。
medium	（任意）電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。

コマンド デフォルト

EDRRM は無効で、感度は low です。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

感度を設定する前に EDRRM を有効にする必要があります。

次に、デフォルトの EDRRM の状態と感度を設定する例を示します。

```
Device(config)# default ap dot11 5ghz rrm channel cleanair-event
Device(config)# default ap dot11 5ghz rrm channel cleanair-event sensitivity
```

default ap dot11 5ghz rrm channel device

802.11a チャネルに永続的非 WiFi デバイスの回避のデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **default apdot115ghzrrmchannel device** コマンドを使用します。

default ap dot11 5ghz rrm channel device

構文の説明

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

永続的デバイスの状態は無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、802.11a チャネルに永続的非 WiFi デバイスの回避を設定する例を示します。

```
Device(config)# default ap dot11 5ghz rrm channel device
```

default ap dot11 24ghz cleanair alarm device

2.4 GHz 干渉デバイスのアラームのデフォルト値を設定するには、グローバル コンフィギュレーション モードで **default apdot1124ghzcleanairalarmdevice** コマンドを使用します。

default ap dot11 24ghz cleanair alarm device {**bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like | fh**| **inv**| **jammer | mw-oven**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**}

構文の説明

bt-discovery	Bluetooth 干渉デバイスのアラームを設定します。
bt-link	任意の Bluetooth リンクのアラームを設定します。
canopy	canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）と同様の電話機のアラームを設定します。
fh	802.11 周波数ホッピング（FH）デバイスのアラームを設定します。
inv	スペクトラム反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害装置干渉デバイスのアラームを設定します。
mw-oven	電子レンジのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。

video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。
xbox	Xbox 干渉デバイスのアラームを設定します。
zigbee	802.15.4 干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi反転デバイスのアラームは有効になっています。その他のデバイスのアラームはすべて無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、デフォルトの CleanAir 2.4 GHz 干渉デバイスのアラームを設定する例を示します。

```
Device(config)# default ap dot11 24ghz cleanair alarm device inv
```

default ap dot11 24ghz cleanair device

2.4 GHz干渉デバイスのレポート生成のデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **defaultapdot1124ghzcleanairdevice** コマンドを使用します。

default ap dot11 24ghz cleanair device {**ble-beacon**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fh**| **inv**| **jammer**| **mw-oven**| **nonstd**| **report**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**}

構文の説明

ble-beacon	BLE ビーコン機能を設定します。
bt-discovery	Bluetooth 干渉デバイスのアラームを設定します。
bt-link	任意の Bluetooth リンクのアラームを設定します。
canopy	canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）と同様の電話機のアラームを設定します。
fh	802.11 周波数ホッピングデバイスのアラームを設定します。
inv	スペクトラム反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害装置干渉デバイスのアラームを設定します。
mw-oven	電子レンジのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。

video	ビデオカメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。
xbox	Xbox 干渉デバイスのアラームを設定します。
zigbee	802.15.4 干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi反転デバイスのアラームは有効になっています。その他のデバイスのアラームはすべて無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	このコマンドが変更されました。**ble-beacon** キーワードが追加されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、CleanAir によるビデオ カメラの干渉時のレポートを有効にする例を示します。

```
Device(config)# default ap dot11 24ghz cleanair device video
```

関連トピック

ap dot11 24ghz cleanair, （39 ページ）
ap dot11 24ghz cleanair alarm air-quality, （40 ページ）
ap dot11 24ghz cleanair alarm device, （41 ページ）

default ap dot11 24ghz rrm channel cleanair-event

2.4 GHz デバイスのデフォルトのイベント駆動型無線リソース管理（EDRRM）の状態と感度を設定するには、グローバル コンフィギュレーション モードで **default apdot1124ghzrrmchannelcleanair-event** コマンドを使用します。

default ap dot11 24ghz rrm channel cleanair-event [**sensitivity** {**high**| **low**| **medium**}]

構文の説明

sensitivity	CleanAir イベントの EDRRM 感度を設定します。
high	電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。
low	電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。
medium	電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。

コマンド デフォルト

EDRRM は無効で、感度は low です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、EDRRM を有効にし、デフォルトの EDRRM 感度を設定する例を示します。

```
Device(config)# default ap dot11 24ghz rrm channel cleanair-event
Device(config)# default ap dot11 24ghz rrm channel cleanair-event sensitivity
```

show ap dot11 5ghz cleanair air-quality summary

5 GHz 帯域の CleanAir AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 5ghz cleanair air-quality summary** コマンドを使用します。

show ap dot11 5ghz cleanair air-quality summary

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、5 GHz 帯域の CleanAir AQ データを表示する例を示します。

```
Device# show ap dot11 5ghz cleanair air-quality summary

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name              Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP270ca.9b86.4546    1         99      99      0            No
AP2894.0f26.22df     6         98      97      0            No
AP2894.0f58.cc6b     11        99      99      0            No
AP2894.0f39.1040     6         97      97      0            No
AP2894.0f63.c6da     11        99      99      0            No
AP2894.0f58.d013     6         97      97      0            No
```

show ap dot11 5ghz cleanair air-quality worst

5 GHz 帯域の最も深刻な AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 5ghz cleanair air-quality worst** コマンドを使用します。

show ap dot11 5ghz cleanair air-quality worst

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、5 GHz 帯域の最も深刻な AQ データを表示する例を示します。

```
Device# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-------------------------------------------------------------
AP2894.0f39.1040    6         97      97      0            No
```

show ap dot11 5ghz cleanair config

5 GHz 帯域の CleanAir 設定を表示するには、**show ap dot11 5ghz cleanair config** コマンドを使用します。

show ap dot11 5ghz cleanair config

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

リリース 3.3 SE では、モビリティ エージェント（MA）でこのコマンドを設定できます。

次に、モビリティ コントローラ上の 5 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Device# show ap dot11 5ghz cleanair config
```

```
CleanAir Solution..............................  : Enabled
Air Quality Settings:
    Air Quality Reporting......................  : Enabled
    Air Quality Reporting Period (min).........  : 15
    Air Quality Alarms.........................  : Enabled
    Air Quality Alarm Threshold................  : 1
Interference Device Settings:
    Interference Device Reporting..............  : Enabled
        TDD Transmitter........................  : Enabled
        Jammer.................................  : Enabled
        Continuous Transmitter.................  : Enabled
        DECT-like Phone........................  : Enabled
        Video Camera...........................  : Enabled
        WiFi Inverted..........................  : Enabled
        WiFi Invalid Channel...................  : Enabled
        SuperAG................................  : Enabled
        Canopy.................................  : Enabled
        WiMax Mobile...........................  : Enabled
        WiMax Fixed............................  : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter........................  : Enabled
        Jammer.................................  : Enabled
        Continuous Transmitter.................  : Enabled
        DECT-like Phone........................  : Enabled
        Video Camera...........................  : Enabled
        WiFi Inverted..........................  : Enabled
        WiFi Invalid Channel...................  : Enabled
        SuperAG................................  : Enabled
        Canopy.................................  : Enabled
        WiMax Mobile...........................  : Enabled
        WiMax Fixed............................  : Enabled
    Interference Device Alarms.................  : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State............  : Enabled
    CleanAir Driven RRM Sensitivity............  : HIGH
    CleanAir Persistent Devices state..........  : Enabled
```

次に、モビリティ エージェント上の 5 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Device# show ap dot11 5ghz cleanair config

Mobility Controller Link Status................  : UP
CleanAir Solution..............................  : Enabled
Air Quality Settings:
    Air Quality Reporting......................  : Enabled
    Air Quality Reporting Period (min).........  : 15
    Air Quality Alarms.........................  : Enabled
    Air Quality Alarm Threshold................  : 10
Interference Device Settings:
    Interference Device Reporting..............  : Enabled
        TDD Transmitter........................  : Enabled
        Jammer.................................  : Enabled
        Continuous Transmitter.................  : Enabled
        DECT-like Phone........................  : Enabled
        Video Camera...........................  : Enabled
        WiFi Inverted..........................  : Enabled
        WiFi Invalid Channel...................  : Enabled
        SuperAG................................  : Enabled
        Canopy.................................  : Enabled
        WiMax Mobile...........................  : Enabled
        WiMax Fixed............................  : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter........................  : Disabled
        Jammer.................................  : Disabled
        Continuous Transmitter.................  : Disabled
        DECT-like Phone........................  : Disabled
        Video Camera...........................  : Disabled
        WiFi Inverted..........................  : Enabled
        WiFi Invalid Channel...................  : Enabled
        SuperAG................................  : Enabled
        Canopy.................................  : Disabled
        WiMax Mobile...........................  : Disabled
        WiMax Fixed............................  : Disabled
```

```
    Interference Device Alarms.................. : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State............. : Disabled
    CleanAir Driven RRM Sensitivity............. : LOW
    CleanAir Persistent Devices state........... : Disabled
```

show ap dot11 5ghz cleanair device type

5 GHz 干渉源デバイスを表示するには、**showapdot115ghzcleanairdevicetype** コマンドを使用します。

show ap dot11 5ghz cleanair device type {**all**| **canopy**| **cont-tx**| **dect-like**| **inv**| **jammer**| **nonstd**| **persistent**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**}

構文の説明

all	5 GHz 帯域のすべての CleanAir 干渉源デバイスを表示します。
canopy	5 GHz 帯域の canopy タイプの CleanAir 干渉源を表示します。
cont-tx	5 GHz 帯域の continuous transmitter タイプの CleanAir 干渉源を表示します。
dect-like	5 GHz 帯域の Digital Enhanced Cordless Communication（DECT）と同様の電話機タイプの CleanAir 干渉源を表示します。
inv	5 GHz 帯域のスペクトラム反転 WiFi 信号を使用している CleanAir 干渉源デバイスを表示します。
jammer	5 GHz 帯域の jammer タイプの CleanAir 干渉源を表示します。
nonstd	5 GHz 帯域の非標準 Wi-Fi チャネルを使用している CleanAir 干渉源デバイスを表示します。
persistent	5 GHz 帯域の CleanAir 永続型デバイスの干渉源を表示します。
superag	5 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します
tdd-tx	5 GHz 帯域の CleanAir 時分割複信（TDD）トランスミッタを表示します。
video	5 GHz 帯域の video camera タイプの CleanAir 干渉源を表示します。
wimax-fixed	5 GHz 帯域の WiMax fixed タイプの CleanAir 干渉源を表示します。
wimax-mobile	5 GHz 帯域の WiMax mobile タイプの CleanAir 干渉源を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

干渉源デバイスは、5 GHz デバイスから干渉がある場合にのみ表示されます。

次に、すべての 5 GHz 干渉源デバイスを表示する例を示します。

```
Device# show ap dot11 5ghz cleanair device type all

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No    ClusterID          DevID  Type           AP Name                 ISI  RSSI  DC
Channel
-------------------------------------------------------------------------------------------
```

show ap dot11 24ghz cleanair air-quality summary

2.4 GHz 帯域の CleanAir AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 24ghz cleanair air-quality summary** コマンドを使用します。

show ap dot11 24ghz cleanair air-quality summary

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz 帯域の CleanAir AQ データを表示する例を示します。

```
Device# show ap dot11 24ghz cleanair air-quality summary

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP270ca.9b86.4546   1         99      99      0            No
AP2894.0f26.22df    6         98      97      0            No
AP2894.0f58.cc6b    11        99      99      0            No
AP2894.0f39.1040    6         97      97      0            No
AP2894.0f63.c6da    11        99      99      0            No
```

show ap dot11 24ghz cleanair air-quality worst

2.4 GHz 帯域の最も深刻な AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 24ghz cleanair air-quality worst** コマンドを使用します。

show ap dot11 24ghz cleanair air-quality worst

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz 帯域の最も深刻な AQ データを表示する例を示します。

```
Device# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP2895.0f39.1040    6         97      97      0            No
```

show ap dot11 24ghz cleanair config

2.4 GHz 帯域の CleanAir AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 24ghz cleanair config** コマンドを使用します。

show ap dot11 24ghz cleanair config

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

リリース 3.3 SE では、モビリティ エージェント（MA）でこのコマンドを設定できます。

次に、モビリティ コントローラ上の 2.4 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Device# show ap dot11 24ghz cleanair config

CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 1
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Enabled
    CleanAir Driven RRM Sensitivity.............. : HIGH
    CleanAir Persistent Devices state............ : Enabled
```

次に、モビリティ エージェント上の 2.4 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Device# show ap dot11 24ghz cleanair config

Mobility Controller Link Status.................. : UP
CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 10
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Disabled
        Jammer................................... : Disabled
        Continuous Transmitter................... : Disabled
        DECT-like Phone.......................... : Disabled
        Video Camera............................. : Disabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Disabled
        WiMax Mobile............................. : Disabled
        WiMax Fixed.............................. : Disabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Disabled
    CleanAir Driven RRM Sensitivity.............. : LOW
    CleanAir Persistent Devices state............ : Disabled
```

show ap dot11 24ghz cleanair summary

2.4 GHz CleanAir デバイスのサマリーを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showapdot1124ghzcleanairsummary** コマンドを使用します。

showap dot11 24ghz cleanair summary

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show ap dot11 24ghz cleanair summary** コマンドの出力例を示します。

```
Device# show ap dot11 24ghz cleanair summary

AP Name               MAC Address         Slot ID  Spectrum Capable  Spectrum Intelligence
   Spectrum Oper State
-------------------------------------------------------------------------------------------------
AP1cdf.0f95.1719      0817.35c7.1a60            0  Disabled          Disabled
   Down
AS-5508-5-AP3         0817.35dd.9f40            0  Disabled          Disabled
   Down
AP270ca.9b86.4546     0c85.259e.c350            0  Enabled           Enabled
   Up
AP2894.0f26.22df      0c85.25ab.cca0            0  Enabled           Enabled
   Up
AP2894.0f58.cc6b      0c85.25c7.b7a0            0  Enabled           Enabled
   Up
AP2894.0f39.1040      0c85.25de.2c10            0  Enabled           Enabled
   Up
AP2894.0f63.c6da      0c85.25de.c8e0            0  Enabled           Enabled
   Up
```

第 III 部

Flexible NetFlow コマンド

- Flexible NetFlow コマンド，67 ページ

第 4 章

Flexible NetFlow コマンド

- cache, 69 ページ
- clear flow exporter, 71 ページ
- clear flow monitor, 72 ページ
- collect, 74 ページ
- collect counter, 75 ページ
- collect interface, 76 ページ
- collect timestamp absolute, 77 ページ
- collect transport tcp flags, 79 ページ
- datalink flow monitor, 80 ページ
- debug flow exporter, 81 ページ
- debug flow monitor, 82 ページ
- debug flow record, 83 ページ
- debug sampler, 84 ページ
- description, 85 ページ
- destination, 86 ページ
- dscp, 87 ページ
- export-protocol netflow-v9, 88 ページ
- exporter, 89 ページ
- フロー エクスポータ, 90 ページ
- フロー モニタ, 91 ページ
- flow record, 92 ページ

- ip flow monitor, 93 ページ
- ipv6 flow monitor, 95 ページ
- match datalink ethertype, 96 ページ
- match datalink mac, 98 ページ
- match datalink vlan, 99 ページ
- match flow cts, 100 ページ
- match flow direction, 101 ページ
- match interface, 102 ページ
- match ipv4, 103 ページ
- match ipv4 destination address, 104 ページ
- match ipv4 source address, 105 ページ
- match ipv4 ttl, 106 ページ
- match ipv6, 107 ページ
- match ipv6 destination address, 108 ページ
- match ipv6 hop-limit, 109 ページ
- match ipv6 source address, 110 ページ
- match transport, 111 ページ
- match transport icmp ipv4, 112 ページ
- match transport icmp ipv6, 113 ページ
- mode random 1 out-of, 115 ページ
- オプション, 116 ページ
- record, 117 ページ
- sampler, 118 ページ
- show flow exporter, 120 ページ
- show flow interface, 122 ページ
- show flow monitor, 124 ページ
- show flow record, 129 ページ
- show sampler, 130 ページ
- source, 132 ページ
- template data timeout, 134 ページ
- transport, 135 ページ

• ttl, 136 ページ

cache

フロー モニタのフロー キャッシュ パラメータを設定するには、フロー モニタ コンフィギュレーション モードで **cache** コマンドを使用します。フロー モニタのフロー キャッシュ 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。

cache {**timeout** {**active**| **inactive**} *seconds*| **type normal**}

no cache {**timeout** {**active**| **inactive**} | **type**}

構文の説明

timeout	フロー タイムアウトを指定します。
active	アクティブ フロー タイムアウトを指定します。
inactive	非アクティブ フロー タイムアウトを指定します。
seconds	タイムアウト値（秒単位）。範囲は 1 ～ 604800 （7日）です。
type	フロー キャッシュのタイプを指定します。
normal	通常キャッシュ タイプを設定します。フロー キャッシュ内のエントリは、**timeout active** *seconds* および **timeout inactive** *seconds* の設定に従って期限切れになります。これがデフォルトのキャッシュ タイプです。

コマンド デフォルト

デフォルトのフロー モニタ フロー キャッシュ パラメータが使用されます。

フロー モニタの以下のフロー キャッシュ パラメータがイネーブルになっています。

- キャッシュタイプ：normal
- アクティブ フロー タイムアウト：1800 秒
- 非アクティブ フロー タイムアウト：15 秒

コマンド モード

フロー モニタ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

各フロー モニタには、モニタするすべてのフローの保存に使用するキャッシュがあります。各キャッシュには、フローがキャッシュ内に留まることができる時間など、設定可能な要素があります。フローがタイムアウトするとキャッシュから削除され、対応するフロー モニタ用に設定されている任意のエクスポータに送信されます。

cache timeout active コマンドでは、通常タイプのキャッシュのエージング動作を制御します。フローが長時間アクティブになっている場合、通常はエージ アウト（そのフローの後続のパケット用の新しいフローを開始）することが望まれます。このエージアウトプロセスを行うことで、エクスポートを受信するモニタリング アプリケーションに最新の情報を反映し続けることができます。デフォルトでは、このタイムアウトは1800秒（30分）ですが、システム要件に応じて調整できます。大きい値を設定すると、存続時間の長いフローを単一のフロー レコードに記録することができます。小さい値を設定すると、存続時間の長い新しいフローが開始されてから、そのフローのデータがエクスポートされるまでの遅延が短縮されます。アクティブ フロータイムアウトを変更した場合、新しいタイムアウト値はただちに有効になります。

また、**cache timeout inactive** コマンドでも、通常タイプのキャッシュのエージング動作を制御できます。指定した時間内にフローでアクティビティが検出されない場合、そのフローはエージ アウトされます。デフォルトでは、このタイムアウトは15秒ですが、この値は想定されるトラフィックのタイプに応じて調整できます。存続時間の短いフローが多数存在し、多くのキャッシュ エントリが消費されている場合は、非アクティブ タイムアウトを短縮することでこのオーバーヘッドを削減できます。多数のフローが、データを収集し終わる前に頻繁にエージ アウトしている場合は、このタイムアウトを延長することでフローの相関関係を向上できます。非アクティブ フロータイムアウトを変更した場合、新しいタイムアウト値はただちに有効になります。

cache type normal コマンドでは、通常キャッシュ タイプを指定します。これがデフォルトのキャッシュ タイプです。キャッシュのエントリは、**timeout active** *seconds* および **timeout inactive** *seconds* の設定に従って、エージアウトされます。キャッシュ エントリはエージアウトされると、キャッシュから削除され、そのキャッシュに対応するモニタ用に設定されているエクスポータによってエクスポートされます。

キャッシュをデフォルト設定に戻すには、**default cache** フロー モニタ コンフィギュレーション コマンドを使用します。

（注） キャッシュが一杯になると、新しいフローはモニタされません。

次に、フロー モニタ キャッシュのアクティブ タイムアウトを設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout active 4800
```

次に、フロー モニタ キャッシュの非アクティブ タイマーを設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout inactive 30
```

次に、通常キャッシュを設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache type normal
```

関連トピック

フロー モニタ, （91 ページ）

clear flow exporter

Flexible NetFlow フロー エクスポータの統計情報をクリアするには、特権 EXEC モードで **clearflowexporter** コマンドを使用します。

clear flow exporter [[**name**] *exporter-name*] **statistics**

構文の説明

name	（任意）フロー エクスポータの名前を指定します。
exporter-name	（任意）以前に設定されたフロー エクスポータの名前。
statistics	フロー エクスポータの統計情報をクリアします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

clearflowexporter コマンドは、フロー エクスポータからすべての統計情報を削除します。これらの統計情報はエクスポートされず、キャッシュ内に保存されていたデータは失われます。

show flow exporter statistics 特権 EXEC コマンドを使用して、フロー エクスポータの統計情報を表示できます。

次の例では、デバイス で設定されているすべてのフロー エクスポータの統計情報をクリアします。

```
Device# clear flow exporter statistics
```

次の例では、FLOW-EXPORTER-1 という名前のフロー エクスポータの統計情報をクリアします。

```
Device# clear flow exporter FLOW-EXPORTER-1 statistics
```

関連トピック

debug flow exporter, （81 ページ）

show flow exporter, （120 ページ）

clear flow monitor

フロー モニタ キャッシュまたはフロー モニタ統計情報をクリアし、フロー モニタ キャッシュ内のデータを強制的にエクスポートするには、特権 EXEC モードで **clearflowmonitor** コマンドを使用します。

clear flow monitor [**name**] *monitor-name* [[**cache**] **force-export**| **statistics**]

構文の説明

name	フロー モニタの名前を指定します。
monitor-name	以前に設定されたフロー モニタの名前
cache	（任意）フロー モニタ キャッシュ情報をクリアします。
force-export	（任意）フローモニタ キャッシュ統計情報を強制的にエクスポートします。
statistics	（任意）フロー モニタの統計情報をクリアします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

clearflowmonitorcache コマンドを実行すると、フローモニタ キャッシュからすべてのエントリが削除されます。キャッシュ内のエントリはエクスポートされ、キャッシュ内に保存されていたデータは失われます。

（注） クリアされたキャッシュ エントリの統計情報は保持されます。

clearflowmonitorforce-export コマンドを実行すると、フロー モニタ キャッシュからすべてのエントリが削除され、それらのエントリはフローモニタに割り当てられているすべてのフローエクスポータを使用してエクスポートされます。このアクションにより、CPU 使用率は一時的に増加します。このコマンドの使用には注意が必要です。

clearflowmonitorstatistics コマンドを実行すると、このフロー モニタの統計情報がクリアされます。

（注） **clearflowmonitorstatistics** コマンドを実行しても、現在のエントリに関する統計情報はクリアされません。なぜなら、この情報はキャッシュ内に保存されているエントリ数のインジケータであり、キャッシュは、このコマンドによってクリアされないためです。

フロー モニタの統計情報を表示するには、**show flow monitor statistics** 特権 EXEC コマンドを使用します。

次に、FLOW-MONITOR-1 という名前のフロー モニタの統計情報とキャッシュ エントリをクリアする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1
```

次に、FLOW-MONITOR-1 という名前のフロー モニタの統計情報とキャッシュ エントリをクリアして、強制的にエクスポートする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 force-export
```

次に、FLOW-MONITOR-1 という名前のフロー モニタのキャッシュをクリアして、強制的にエクスポートする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 cache force-export
```

次に、FLOW-MONITOR-1 という名前のフロー モニタの統計情報をクリアする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 statistics
```

関連トピック

debug flow monitor, （82 ページ）

show flow monitor, （124 ページ）

collect

フロー モニタ レコードの非キー フィールドを設定し、そのレコードによって作成されたフローの各フィールドへの値の取り込みを有効にするには、フロー レコード コンフィギュレーション モードで **collect** コマンドを使用します。

collect {**counter**| **interface**| **timestamp**| **transport**}

構文の説明

counter	フロー レコードの非キー フィールドとしてフロー内のバイト数またはパケット数を設定します。詳細については、collect counter, （75 ページ）を参照してください。
interface	入力および出力インターフェイス名をフロー レコードの非キー フィールドとして設定します。詳細については、collect interface, （76 ページ）を参照してください。
timestamp	フロー内の最初または最後に確認されたパケットの絶対時間をフロー レコードの非キー フィールドとして設定します。詳細については、collect timestamp absolute, （77 ページ）を参照してください。
transport	フロー レコードからの転送 TCP フラグの収集を有効にします。詳細については、collect transport tcp flags, （79 ページ）を参照してください。

コマンド デフォルト

フロー モニタ レコードの非キー フィールドは設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

非キー フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キー フィールドの値の変更によって新しいフローが作成されることはありませ

ん。ほとんどの場合、非キー フィールドの値はフロー内の最初のパケットからのみ取得されます。

collect コマンドは、フロー モニタ レコードの非キー フィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キー フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キー フィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キー フィールドの値はフロー内の最初のパケットからのみ取得されます。

（注） **flow username** 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。

次に、フローの合計バイト数を非キー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter bytes long
```

関連トピック

collect counter, （75 ページ）

collect interface, （76 ページ）

collect timestamp absolute, （77 ページ）

collect transport tcp flags, （79 ページ）

collect counter

フロー レコードの非キー フィールドとしてフロー内のバイト数またはパケット数を設定するには、フロー レコード コンフィギュレーション モードで **collectcounter** コマンドを使用します。フロー（カウンタ）内のバイト数またはパケット数をフロー レコードの非キーフィールドとして使用する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。

collect counter {**bytes layer2 long**| **bytes long**| **packets long**}

no collect counter {**bytes layer2 long**| **bytes long**| **packets long**}

構文の説明

bytes layer2 long	フローで確認されるレイヤ 2 のバイト数を非キー フィールドとして設定し、64 ビット カウンタを使用してフローからレイヤ 2 の合計バイト数を収集します。
bytes long	フローで確認されるバイト数を非キー フィールドとして設定し、64 ビット カウンタを使用してフローから合計バイト数を収集します。
packets long	フローで確認されるパケット数を非キー フィールドとして設定し、64 ビット カウンタを使用してフローから合計パケット数を収集します。

コマンド デフォルト

フロー内のバイト数またはパケット数は、非キー フィールドとして設定されません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

collect counter bytes long コマンドは、フローで確認されるバイト数の 64 ビット カウンタを設定します。

collect counter packets long コマンドは、フローでパケットが確認されるたびに増分される 64 ビットのカウンタを設定します。64 ビットのカウンタが 0 に戻って再びカウントを開始することはまず考えられません。

このコマンドをデフォルト設定に戻すには、**no collect counter** または **default collect counter** フロー レコード コンフィギュレーション コマンドを使用します。

次に、フローの合計バイト数を非キー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

次に、フローからの合計パケット数を非キー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

関連トピック

flow record, （92 ページ）

collect interface

フロー レコードの非キー フィールドとして入力インターフェイス名を設定するには、フロー レコード コンフィギュレーション モードで **collectinterface** コマンドを使用します。入力インターフェイスをフロー レコードの非キー フィールドとして使用する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。

collect interface input

no collect interface input

構文の説明

input	入力インターフェイス名を非キー フィールドとして設定し、フローから入力インターフェイスを収集します。

コマンド デフォルト

入力インターフェイス名は、非キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

Flexible NetFlow**collect** コマンドは、フロー モニタ レコードの非キー フィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キー フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キー フィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キー フィールドの値はフロー内の最初のパケットからのみ取得されます。

このコマンドをデフォルト設定に戻すには、**no collect interface** または **default collect interface** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、非キー フィールドとして入力インターフェイスを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect interface input
```

関連トピック

フロー エクスポータ, （90 ページ）

flow record, （92 ページ）

collect timestamp absolute

フロー内の最初または最後に確認されたパケットの絶対時間をフロー レコードの非キー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **collecttimestamp**

absolute コマンドを使用します。フロー内の最初または最後に確認されたパケットをフロー レコードの非キー フィールドとして使用するのを無効にするには、このコマンドの **no** 形式を使用します。

collect timestamp absolute {**first**| **last**}

no collect timestamp absolute {**first**| **last**}

構文の説明

first	フロー内の最初に確認されたパケットの絶対時間を非キー フィールドとして設定し、フローからのタイムスタンプの収集を有効にします。
last	フロー内の最後に確認されたパケットの絶対時間を非キー フィールドとして設定し、フローからのタイムスタンプの収集を有効にします。

コマンド デフォルト

絶対時間フィールドは非キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

collect コマンドは、フロー モニタ レコードの非キー フィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キー フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キー フィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キー フィールドの値はフロー内の最初のパケットからのみ取得されます。

次に、フロー内の最初に確認されたパケットの絶対時間に基づくタイムスタンプを非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute first
```

次に、フロー内の最後に確認されたパケットの絶対時間に基づくタイムスタンプを非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute last
```

関連トピック

flow record, （92 ページ）

collect transport tcp flags

フローからの転送TCPフラグの収集をイネーブルにするには、フロー レコードコンフィギュレーション モードで **collecttransporttcpflags** コマンドを使用します。フローからの転送 TCP フラグの収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

collect transport tcp flags

no collect transport tcp flags

構文の説明

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

トランスポート層フィールドは非キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

トランスポート層フィールドの値は、フロー内のすべてのパケットから取得されます。収集するTCP フラグを指定することはできません。転送 TCP フラグの収集のみ指定できます。すべてのTCP フラグはこのコマンドで収集されます。次の転送 TCP フラグを収集します。

- **ack**：TCP 確認応答フラグ
- **cwr**：TCP 輻輳ウィンドウ縮小フラグ
- **ece**：TCP ECN エコー フラグ

- **fin**：TCP 終了フラグ
- **psh**：TCP プッシュ フラグ
- **rst**：TCP リセット フラグ
- **syn**：TCP 同期フラグ
- **urg**：TCP 緊急フラグ

このコマンドをデフォルト設定に戻すには、**no collect collect transport tcp flags** または **default collect collect transport tcp flags** フロー レコード コンフィギュレーション コマンドを使用します。

次に、フローから TCP フラグを収集する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect transport tcp flags
```

関連トピック

flow record, （92 ページ）

datalink flow monitor

インターフェイスに Flexible NetFlow フロー モニタを適用するには、インターフェイス コンフィギュレーション モードで **datalink flow monitor** コマンドを使用します。Flexible NetFlow フロー モニタをディセーブルにするには、このコマンドの **no** 形式を使用します。

datalink flow monitor *monitor-name* **sampler** *sampler-name* **input**

no datalink flow monitor *monitor-name* **sampler** *sampler-name* **input**

構文の説明

monitor-name	インターフェイスに適用するフロー モニタの名前。
sampler *sampler-name*	フロー モニタ用に指定したフロー サンプラーをイネーブルにします。
input	スイッチがインターフェイスで受信するトラフィックをモニタします。

コマンド デフォルト

フロー モニタはイネーブルになっていません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

datalink flow monitor コマンドを使用してインターフェイスにフローモニタを適用する前に、**flow monitor** グローバル コンフィギュレーション コマンドを使用してフローモニタを作成し、**sampler** 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ロー サンプラーを作成しておく必要があります。

フローモニタ用のフローサンプラーをイネーブルにするには、事前にサンプラーを作成しておく必要があります。

（注） **datalink flow monitor** コマンドは、非 IPv4 および非 IPv6 トラフィックだけをモニタします。IPv4 トラフィックをモニタするには、**ip flow monitor** コマンドを使用します。IPv6 トラフィックをモニタするには、**ipv6 flow monitor** コマンドを使用します。

次に、インターフェイス上での Flexible NetFlow データリンク モニタリングをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# datalink flow monitor FLOW-MONITOR-1 sampler FLOW-SAMPLER-1 input
```

関連トピック

フロー モニタ，（91 ページ）

debug flow exporter

Flexible NetFlow フロー エクスポータのデバッグ出力を有効にするには、特権 EXEC モードで **debugflowexporter** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug flow exporter [[**name**] *exporter-name*] [**error**| **event**| **packets** *number*]

no debug flow exporter [[**name**] *exporter-name*] [**error**| **event**| **packets** *number*]

構文の説明

name	（任意）フロー エクスポータの名前を指定します。
exporter-name	（任意）前に設定されたフロー エクスポータの名前。

error	（任意）フローエクスポータのエラーのデバッグをイネーブルにします。
event	（任意）フロー エクスポータのイベントのデバッグをイネーブルにします。
packets	（任意）フロー エクスポータのパケットレベルのデバッグをイネーブルにします。
number	（任意）フロー エクスポータのパケットレベルのデバッグでデバッグするパケット数。指定できる範囲は 1 ～ 65535 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例は、フロー エクスポータのパケットがプロセス送信用のキューに格納されたことを示しています。

```
Device# debug flow exporter
May 21 21:29:12.603: FLOW EXP: Packet queued for process send
```

関連トピック

clear flow exporter, （71 ページ）

debug flow monitor

Flexible NetFlow フロー モニタのデバッグ出力を有効にするには、特権 EXEC モードで **debugflowmonitor** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug flow monitor [**error**| [**name**] *monitor-name* [**cache** [**error**]| **error**| **packets** *packets*]]

no debug flow monitor [**error**| [**name**] *monitor-name* [**cache** [**error**]| **error**| **packets** *packets*]]

構文の説明

error	（任意）すべてのフロー モニタまたは指定されたフロー モニタのフロー モニタ エラーのデバッグをイネーブルにします。
name	（任意）フロー モニタの名前を指定します。

monitor-name	（任意）事前に設定されたフロー モニタの名前。
cache	（任意）フロー モニタ キャッシュのデバッグをイネーブルにします。
cache error	（任意）フローモニタ キャッシュ エラーのデバッグをイネーブルにします。
packets	（任意）フロー モニタのパケットレベルのデバッグをイネーブルにします。
packets	（任意）フローモニタのパケットレベルのデバッグでデバッグするパケットの数。指定できる範囲は 1 ～ 65535 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例は、FLOW-MONITOR-1 のキャッシュが削除されたことを示しています。

```
Device# debug flow monitor FLOW-MONITOR-1 cache
May 21 21:53:02.839: FLOW MON:  'FLOW-MONITOR-1' deleted cache
```

関連トピック

clear flow monitor, （72 ページ）

debug flow record

Flexible NetFlow フロー レコードのデバッグ出力を有効にするには、特権 EXEC モードで **debugflowrecord** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug flow record [[**name**] *record-name*| **options** {**sampler-table**}| [**detailed**| **error**]]

no debug flow record [[**name**] *record-name*| **options** {**sampler-table**}| [**detailed**| **error**]]

構文の説明

name	（任意）フロー レコードの名前を指定します。
record-name	（任意）前に設定されたユーザ定義のフロー レコードの名前。

options	（任意）他のフロー レコード オプションに関する情報が含まれます。
sampler-table	（任意）サンプラー テーブルに関する情報が含まれます。
detailed	（任意）詳細情報を表示します。
error	（任意）エラーのみを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、フロー レコードのデバッグを有効にする例を示します。

```
Device# debug flow record FLOW-record-1
```

debug sampler

Flexible NetFlow サンプラーのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debugsampler** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sampler [**detailed**| **error**| [**name**] *sampler-name* [**detailed**| **error**| **sampling** *samples*]]

no debug sampler [**detailed**| **error**| [**name**] *sampler-name* [**detailed**| **error**| **sampling**]]

構文の説明

detailed	（任意）サンプラー要素の詳細デバッグをイネーブルにします。
error	（任意）サンプラー エラーのデバッグをイネーブルにします。
name	（任意）サンプラーの名前を指定します。
sampler-name	（任意）前に設定されたサンプラーの名前。
sampling*samples*	（任意）サンプリングのデバッグをイネーブルにし、デバッグするサンプルの数を指定します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、デバッグ プロセスが SAMPLER-1 というサンプラーの ID を取得した場合の出力例を示します。

```
Device# debug sampler detailed
*May 28 04:14:30.883: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et1/0,O)
 get ID succeeded:1
*May 28 04:14:30.971: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et0/0,I)
 get ID succeeded:1
```

description

フロー モニタ、フロー エクスポータ、またはフロー レコードの説明を設定するには、該当するコンフィギュレーション モードで **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。

description *description*

no description *description*

構文の説明

description	フロー モニタ、フロー エクスポータ、またはフロー レコードを説明するテキスト文字列。

コマンド デフォルト

フロー サンプラー、フロー モニタ、フロー エクスポータ、またはフロー レコードのデフォルトの説明は「ユーザ定義」です。

コマンド モード

次のコマンド モードがサポートされています。

フロー エクスポータ コンフィギュレーション

フロー モニタ コンフィギュレーション

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、該当するコンフィギュレーション モードで **no description** または **default description** コマンドを使用します。

次に、フロー モニタの説明を設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

関連トピック

フロー エクスポータ，（90 ページ）

フロー モニタ，（91 ページ）

flow record，（92 ページ）

destination

フローエクスポータのエクスポート宛先を設定するには、フローエクスポータ コンフィギュレーション モードで **destination** コマンドを使用します。フロー エクスポータのエクスポート宛先を削除するには、このコマンドの **no** 形式を使用します。

destination {*hostname*| *ip-address*} **vrf** *vrf-label*

no destination {*hostname*| *ip-address*} **vrf** *vrf-label*

構文の説明

hostname	NetFlow 情報を送信するデバイスのホスト名。
ip-address	NetFlow 情報を送信するワークステーションの IPv4 アドレス。
vrf	（任意）エクスポート データ パケットをグローバル ルーティング テーブルではなく、名前付きバーチャル プライベート ネットワーク（VPN ）ルーティングおよび転送（VRF）インスタンスに送信して、宛先にルーティングするように指定します。
vrf-label	VRF インスタンスの名前。

コマンド デフォルト

エクスポート宛先は設定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

各フロー エクスポータには、宛先アドレスまたはホスト名を 1 つのみ指定できます。

デバイスの IP アドレスの代わりに、ホスト名を設定すると、ホスト名は直ちに解決され、IPv4 アドレスが実行コンフィギュレーションに保存されます。ドメイン ネーム システム（DNS）の最初の名前解決に使用されたホスト名と IP アドレスのマッピングが DNS サーバ上で動的に変わる場合は、デバイスでこれが検出されないため、エクスポートされたデータは最初の IP アドレスに送信され続け、データは失われます。

このコマンドをデフォルト設定に戻すには、フロー エクスポータ コンフィギュレーション モードで **no destination** または **default destination** コマンドを使用します。

次の例に、宛先システムに Flexible NetFlow キャッシュ エントリをエクスポートするようにネットワーク デバイスを設定する方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

次の例に、VRF-1 という名前の VRF を使用して宛先システムに Flexible NetFlow キャッシュ エントリをエクスポートするようにネットワーク デバイスを設定する方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 172.16.0.2 vrf VRF-1
```

関連トピック

フロー エクスポータ，（90 ページ）

dscp

フロー エクスポータ データグラムの Differentiated Services Code Point（DSCP; DiffServ コード ポイント）の値を設定するには、フロー エクスポータ コンフィギュレーション モードで **dscp** コマンドを使用します。フロー エクスポータ データグラムの DSCP 値を削除するには、このコマンドの **no** 形式を使用します。

dscp *dscp*

no dscp *dscp*

構文の説明

dscp	エクスポートされたデータグラムの DSCP フィールドで使用される DSCP。指定できる範囲は 0 ～ 63 です。デフォルトは 0 です。

コマンド デフォルト

Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値は 0 です。

コマンド モード

フロー エクスポータ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、**no dscp** または **default dscp** フロー エクスポータ コンフィギュレーション コマンドを使用します。

次に、エクスポートされたデータグラムの DSCP フィールドの値を 22 に設定する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# dscp 22
```

関連トピック

フロー エクスポータ, （90 ページ）

export-protocol netflow-v9

NetFlow バージョン 9 エクスポートを Flexible NetFlow エクスポータのエクスポート プロトコルとして設定するには、フロー エクスポータ コンフィギュレーション モードで **export-protocol netflow-v9** コマンドを使用します。

export-protocol netflow-v9

構文の説明

コマンド デフォルト

このコマンドには引数またはキーワードはありません。

NetFlow エクスポータ 9 がイネーブルです。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デバイスは NetFlow v5 エクスポート フォーマットをサポートしていません。NetFlow v9 エクスポート フォーマットのみがサポートされています。

次の例では、NetFlow バージョン 9 エクスポートを NetFlow エクスポータのエクスポート プロトコルとして設定します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# export-protocol netflow-v9
```

関連トピック

フロー エクスポータ, （90 ページ）

exporter

フロー モニタのフロー エクスポータを追加するには、適切なコンフィギュレーション モードで **exporter** コマンドを使用します。フロー モニタ用のフロー エクスポ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。

exporter *exporter-name*

no exporter *exporter-name*

構文の説明

exporter-name	事前に設定したフロー エクスポータの名前

コマンド デフォルト

エクスポータは設定されていません。

コマンド モード

フロー モニタ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

事前に **flowexporter** コマンドを使用してフロー エクスポータを作成してから、**exporter** コマンドを使用してフロー エクスポータをフロー モニタに適用する必要があります。

このコマンドをデフォルト設定に戻すには、**no exporter** または **default exporter** フロー モニタ コンフィギュレーション コマンドを使用します。

次の例では、フロー モニタのエクスポータを設定します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# exporter EXPORTER-1
```

関連トピック

フロー エクスポータ，（90 ページ）

フロー モニタ，（91 ページ）

フロー エクスポータ

Flexible NetFlow フロー エクスポータを作成するか、既存の Flexible NetFlow フロー エクスポータを変更して、Flexible NetFlow フロー エクスポータ 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 **flowexporter** コマンドを使用します。Flexible NetFlow フロー エクスポ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。

flow exporter *exporter-name*

no flow exporter *exporter-name*

構文の説明

exporter-name	作成または変更するフロー エクスポータの名前。

コマンド デフォルト

Flexible NetFlow フロー エクスポータは、コンフィギュレーション内には存在しません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フローエクスポータでは、フローモニタ キャッシュ内のデータをリモート システム（たとえば、分析および保管のために NetFlow コレクタを実行するサーバ）にエクスポートします。フロー エクスポータは、コンフィギュレーションで別のエンティティとして作成されます。フロー エクスポータは、フロー モニタにデータ エクスポート機能を提供するためにフロー モニタに割り当てられます。複数のフロー エクスポータを作成して、1 つまたは複数のフロー モニタに適用すると、いくつかのエクスポート先を指定することができます。1つのフローエクスポータを作成し、いくつかのフロー モニタに適用することができます。

次に、FLOW-EXPORTER-1 という名前のフロー エクスポータを作成し、Flexible NetFlow フロー エクスポータ コンフィギュレーション モードを開始する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```

関連トピック

clear flow exporter, （71 ページ）

debug flow exporter, （81 ページ）

show flow exporter, （120 ページ）

フロー モニタ

フローモニタを作成するか、または既存のフローモニタを変更して、フローモニタ 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 **flowmonitor** コマンドを使用します。フロー モニタを削除するには、このコマンドの **no** 形式を使用します。

flow monitor *monitor-name*

no flow monitor *monitor-name*

構文の説明

monitor-name	作成または変更するフロー モニタの名前。

コマンド デフォルト

Flexible NetFlow フローモニタはコンフィギュレーション内には存在しません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フローモニタは、ネットワーク トラフィックのモニタリングを実行するためにインターフェイスに適用される Flexible NetFlow コンポーネントです。フロー モニタは、フロー レコードとキャッシュで構成されます。フローモニタを作成した後に、フローモニタにレコードを追加します。フローモニタのキャッシュは、フローモニタが最初のインターフェイスに適用されると自動的に作成されます。フロー データは、モニタリング プロセス中にネットワーク トラフィックから収集されます。このデータ収集は、フローモニタのレコード内のキーフィールドおよび非キーフィールドに基づいて実行され、フロー モニタのキャッシュに保存されます。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタを作成し、フロー モニタ コンフィギュレーション モードを開始します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

関連トピック

clear flow monitor, （72 ページ）

debug flow monitor, （82 ページ）

show flow monitor, （124 ページ）

flow record

Flexible NetFlow フロー レコードを作成するか、既存の Flexible NetFlow フロー レコードを変更して、Flexible NetFlow フロー レコード 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 **flowrecord** コマンドを使用します。Flexible NetFlow レコードを削除するには、このコマンドの **no** 形式を使用します。

flow record *record-name*

no flow record *record-name*

構文の説明

record-name	作成または変更するフロー レコードの名前。

コマンド デフォルト

Flexible NetFlow フロー レコードは設定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードでは、フロー内のパケットを識別するために Flexible NetFlow で使用するキーとともに、Flexible NetFlow がフローについて収集する関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フロー レコードを定義できます。は、幅広いキーセットをサポートします。フロー レコードでは、フロー単位で収集するカウンタのタイプも定義します。64 ビットのパケットまたはバイト カウンタを設定できます。

次に、FLOW-RECORD-1 という名前のフロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```

関連トピック

show flow record, （129 ページ）

ip flow monitor

デバイスが受信する IPv4 トラフィックの Flexible NetFlow フロー モニ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 **ip flow monitor** を使用します。フロー モニタをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

no ip flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

構文の説明

monitor-name	インターフェイスに適用するフロー モニタの名前。
sampler *sampler-name*	（任意）フロー モニタ用に指定したフロー サンプラーの名前をイネーブルにします。
input	デバイスがインターフェイスで受信する IPv4トラフィックをモニタします。

コマンド デフォルト

フロー モニタはイネーブルになっていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 flow monitor コマンドを使用して、任意のインターフェイスにフロー モニタを適用するには、事前に **flow monitor** グローバル コンフィギュレーション コマンドを使用して、フロー モニタを作成しておく必要があります。

フロー モニタにサンプラーを追加すると、その名前付きサンプラーによって選択されたパケットだけがキャッシュに保存され、フローを形成します。サンプラーを使用するたびに、その使用に対応する統計情報が別個に保存されます。

インターフェイスですでにイネーブルになっているフロー モニタにサンプラーを追加することはできません。まず、そのフローモニタをインターフェイスから削除してから、同じフローモニタをサンプラーとともに追加する必要があります。

（注） 想定される使用状況を得るには、各フローの統計情報をスケールする必要があります。たとえば、100 パケットにつき 1 パケットをサンプリングするサンプラーを使用した場合は、パケット カウンタとバイト カウンタを 100 倍する必要があります。

次に、入力トラフィックのモニタリングのためにフロー モニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

次に、サンプラーによってサンプリングされる入力パケット数を制限した状態で、入力トラフィックをモニタするようにフロー モニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

次の例では、サンプラーなしでインターフェイスでイネーブルになっているフロー モニタにサンプラーを追加する場合の動作を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

次の例では、フロー モニタをサンプラーと一緒にイネーブルにできるようにするために、インターフェイスからいったん削除する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

関連トピック

フロー モニタ, （91 ページ）
sampler, （118 ページ）

ipv6 flow monitor

デバイスが受信するIPv6トラフィックのフローモニ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 **ipv6 flow monitor** コマンドを使用します。 フロー モニタをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

no ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

構文の説明

monitor-name	インターフェイスに適用するフロー モニタの名前。
sampler *sampler-name*	（任意）フロー モニタ用に指定したフロー サンプラーの名前をイネーブルにします。
input	デバイスがインターフェイスで受信するIPv6トラフィックをモニタします。

コマンド デフォルト

フロー モニタはイネーブルになっていません。

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
Cisco IOS XE 3.2SE	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 flow monitor コマンドを使用して、フロー モニタをインターフェイスに適用するには、**flow monitor** グローバル コンフィギュレーション コマンドを使用して、フロー モニタを事前に作成しておく必要があります。

フロー モニタにサンプラーを追加すると、その名前付きサンプラーによって選択されたパケットだけがキャッシュに保存され、フローを形成します。サンプラーを使用するたびに、その使用に対応する統計情報が別個に保存されます。

インターフェイスですでにイネーブルになっているフロー モニタにサンプラーを追加することはできません。まず、そのフローモニタをインターフェイスから削除してから、同じフローモニタをサンプラーとともに追加する必要があります。

（注） 想定される使用状況を得るには、各フローの統計情報をスケールする必要があります。たとえば、100 パケットにつき 1 パケットをサンプリングするサンプラーを使用した場合は、パケット カウンタとバイト カウンタを 100 倍する必要があります。

次に、入力トラフィックのモニタリングのためにフロー モニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
```

次に、サンプラーによってサンプリングされる入力パケット数を制限した状態で、入力トラフィックをモニタするようにフロー モニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

次の例では、サンプラーなしでインターフェイスでイネーブルになっているフロー モニタにサンプラーを追加する場合の動作を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

次の例では、フロー モニタをサンプラーと一緒にイネーブルにできるようにするために、インターフェイスからいったん削除する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

関連トピック

フロー モニタ, （91 ページ）

sampler, （118 ページ）

match datalink ethertype

パケットの EtherType をフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match datalink ethertype** コマンドを使用します。パケットの EtherType をフロー レコードのキー フィールドとして使用する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。

match datalink ethertype

no match datalink ethertype

構文の説明

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

パケットの EtherType はキー フィールドとして設定されません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードにキー フィールドが含まれていない場合は、フロー モニタで使用することができません。フローはキーフィールドによって識別され、各フローにはキーフィールド値の一意のセットが含まれています。キー フィールドは、**match** コマンドを使用して定義されます。

match datalink ethertype コマンドを使用して、パケットの EtherType をフロー レコードのキー フィールドとして設定すると、トラフィック フローは、インターフェイスに割り当てられたフロー モニタのタイプに基づいて作成されます。

- **datalink flow monitor** インターフェイス コンフィギュレーション コマンドを使用して、データリンク フロー モニタがインターフェイスに割り当てられると、異なるレイヤ 2 プロトコルに対して一意のフローが作成されます。
- **ip flow monitor** インターフェイス コンフィギュレーション コマンドを使用して、IP フロー モニタがインターフェイスに割り当てられると、異なる IPv4 プロトコルに対して一意のフローが作成されます。
- **ipv6 flow monitor** インターフェイス コンフィギュレーション コマンドを使用して、IPv6 フロー モニタがインターフェイスに割り当てられると、異なる IPv6 プロトコルに対して一意のフローが作成されます。

このコマンドをデフォルトの設定に戻すには、**no match datalink ethertype** または **default match datalink ethertype** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、パケットの EtherType を Flexible NetFlow フロー レコードのキー フィールドとして設定しています。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink ethertype
```

関連トピック

flow record, （92 ページ）

match datalink mac

フロー レコードのキー フィールドとして MAC アドレスを使用するように設定するには、フロー レコード コンフィギュレーション モードで **match datalink mac** コマンドを使用します。フロー レコードのキー フィールドとして MAC アドレスを使用する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。

match datalink mac {**destination address input**| **source address input**}

no match datalink mac {**destination address input**| **source address input**}

構文の説明

destination address	キーフィールドとして宛先MACアドレスを使用するように設定します。
input	入力パケットの MAC アドレスを指定します。
source address	キーフィールドとして送信元MACアドレスを使用するように設定します。

コマンド デフォルト

MAC アドレスは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キーフィールドは、match コマンドを使用して定義されます。

input キーワードを使用して、**match datalink mac** コマンドで使用する観測ポイントを指定し、ネットワーク トラフィックの一意の MAC アドレスに基づいてフローを作成します。

（注） データリンク フロー モニタがインターフェイスまたは VLAN レコードに割り当てられている場合、非 IPv6 または非 IPv4 トラフィック用のフローだけが作成されます。

このコマンドをデフォルト設定に戻すには、**no match datalink mac** または **default match datalink mac** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、フロー レコードのキーフィールドとして、デバイスによって受信されるパケットの宛先 MAC アドレスを使用するように設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink mac destination address input
```

関連トピック

flow record, （92 ページ）

match datalink vlan

VLAN ID をフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match datalink vlan** コマンドを使用します。VLAN ID をフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match datalink vlan input

no match datalink vlan input

構文の説明

input	デバイスが受信しているトラフィックの VLAN ID をキー フィールドとして設定します。

コマンド デフォルト

VLAN ID はキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフローモニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キーフィールドは、match コマンドを使用して定義されます。

input キーワードは **match datalink vlan** コマンドがネットワーク トラフィックに固有の VLAN ID に基づいてフローを作成するための観測点を指定するために使用されます。

次に、デバイスが受信しているトラフィックの VLAN ID をフロー レコードのキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink vlan input
```

関連トピック

flow record, （92 ページ）

match flow cts

フロー レコードの CTS 送信元グループ タグおよび宛先グループ タグを設定するには、フロー レコード コンフィギュレーション モードで **match flow cts** コマンドを使用します。グループ タグをフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match flow cts{**source**| **destination**}**group-tag**

no match flow cts{**source**| **destination**}**group-tag**

構文の説明

cts destination group-tag	CTS 宛先フィールド グループをキー フィールドとして設定します。
cts source group-tag	CTS 送信元フィールド グループをキー フィールドとして設定します。

コマンド デフォルト

CTS 宛先または送信元フィールド グループ、フロー方向およびフロー サンプラー ID は、キー フィールドとして設定されていません。

コマンド モード

Flexible NetFlow フロー レコード コンフィギュレーション（config-flow-record）

ポリシー インライン コンフィギュレーショ（config-if-policy-inline）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.3E	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x ではサポートされていませんでした。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キーフィールドは、match コマンドを使用して定義されます。

次に、送信元グループ タグをキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow cts source group-tag
```

match flow direction

フロー方向をフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーションモードで **match flow direction** コマンドを使用します。フロー方向をフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match flow direction

no match flow direction

構文の説明デフォルト

このコマンドには引数またはキーワードは設定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キーフィールドは、**match** コマンドを使用して定義されます。

match flow direction コマンドは、フローの方向をキー フィールドとしてキャプチャします。この機能は、入力フローと出力フローに対して単一のフロー モニタが設定されている場合に最も役立ちます。また、入力と出力で 1 回ずつ、2 回モニタされているフローを見つけ、除外するために使用することができます。このコマンドは、2 つのフローが反対方向に流れている場合に、エクスポートされたデータ内のフローのペアを一致させるために役立つ場合もあります。

次に、フローがモニタされた方向をキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow direction
```

関連トピック

flow record, （92 ページ）

match interface

入力インターフェイスと出力インターフェイスをフロー レコードのキーフィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match interface** コマンドを使用します。入力インターフェイスと出力インターフェイスをフロー レコードのキーフィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match interface {**input**| **output**}

no match interface {**input**| **output**}

構文の説明

input	入力インターフェイスをキー フィールドとして設定します。
output	出力インターフェイスをキー フィールドとして設定します。

コマンド デフォルト

入力インターフェイスと出力インターフェイスは、キー フィールドとして設定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフローモニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キーフィールドは、match コマンドを使用して定義されます。

次に、入力インターフェイスをキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface input
```

次に、出力インターフェイスをキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface output
```

関連トピック

flow record, （92 ページ）

match ipv4

フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4** コマンドを使用します。フロー レコードのキーフィールドとして 1 つ以上の IPv4 フィールドを使用する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。

match ipv4 {**destination address**| **protocol**| **source address**| **tos**| **ttl**| **version**}

no match ipv4 {**destination address**| **protocol**| **source address**| **tos**| **ttl**| **version**}

構文の説明

destination address	キーフィールドとしてIPv4宛先アドレスを設定します。詳細については、match ipv4 destination address, （104 ページ）を参照してください。
protocol	キー フィールドとして IPv4 プロトコルを設定します。
source address	キーフィールドとしてIPv4宛先アドレスを設定します。詳細については、match ipv4 source address, （105 ページ）を参照してください。
tos	キー フィールドとして IPv4 ToS を設定します。

ttl	フロー レコードのキー フィールドとしてIPv4存続可能時間（TTL）フィールドを設定します。詳細については、match ipv4 ttl, （106 ページ）を参照してください。
version	キー フィールドとして IPv4 ヘッダーの IP バージョンを設定します。

コマンド デフォルト

ユーザ定義のフロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定は、イネーブルになっていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフローモニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キー フィールドは、match コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv4 プロトコルを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 protocol
```

関連トピック

flow record, （92 ページ）

match ipv4 destination address

IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 destination address** コマンドを使用します。IPv4 宛先アドレスをフローレコードのキーフィールドとして使用する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。

match ipv4 destination address

no match ipv4 destination address

構文の説明デフォルト

IPv4 宛先アドレスは引数またはキーフィールドとして設定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードにキー フィールドが含まれていない場合は、フロー モニタで使用することができません。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドで定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 destination address** または **default match ipv4 destination address** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 destination address
```

関連トピック

flow record, （92 ページ）

match ipv4 source address

フロー レコードのキー フィールドとして IPv4 送信元アドレスを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 source address** コマンドを使用します。フロー レコードのキーフィールドとしてIPv4送信元アドレスを使用する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。

match ipv4 source address

no match ipv4 source 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

IPv4 送信元アドレスがキー フィールドとして設定されません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードにキー フィールドが含まれていない場合は、フロー モニタで使用することができません。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 source address** または **default match ipv4 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、キー フィールドとして IPv4 送信元アドレスを設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 source address
```

関連トピック

flow record, （92 ページ）

match ipv4 ttl

フロー レコードのキーフィールドとしてIPv4存続可能時間（TTL）フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 ttl** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 TTL を使用する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。

match ipv4 ttl

no match ipv4 ttl

構文の説明

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

IPv4 存続可能時間（TTL）フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードにキー フィールドが含まれていない場合は、フロー モニタで使用することができません。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キー フィールドは、**match ipv4 ttl** コマンドを使用して定義します。

次に、キー フィールドとして IPv4 TTL を設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 ttl
```

関連トピック

flow record, （92 ページ）

match ipv6

フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを使用する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。

match ipv6 {**destination address**| **hop-limit**| **protocol**| **source address**| **traffic-class**| **version**}

no match ipv6 {**destination address**| **hop-limit**| **protocol**| **source address**| **traffic-class**| **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 destination address, （108 ページ）を参照してください。
hop-limit	キー フィールドとして IPv6 ホップ リミットを設定します。詳細については、match ipv6 hop-limit, （109 ページ）を参照してください。
protocol	キー フィールドとして IPv6 プロトコルを設定します。

source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、 match ipv6 source address, （110 ページ）を参照してください。
traffic-class	キー フィールドとして IPv6 トラフィック クラスを設定します。
version	キー フィールドとして IPv6 ヘッダーの IPv6 バージョンを設定します。

コマンド デフォルト

IPv6 の各フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv6 プロトコル フィールドを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 protocol
```

関連トピック

flow record, （92 ページ）

match ipv6 destination address

フロー レコードのキー フィールドとして IPv6 宛先アドレスを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 destination address** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 宛先アドレスを使用する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。

match ipv6 destination address

no match ipv6 destination 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

IPv6 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キーフィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 destination address** または **default match ipv6 destination address** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、キー フィールドとして IPv6 宛先アドレスを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 destination address
```

関連トピック

flow record, （92 ページ）

match ipv6 hop-limit

フロー レコードのキー フィールドとして IPv6 ホップ リミットを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 hop-limit** コマンドを使用します。フロー レコードのキーフィールドとしてIPv6パケットのセクションを使用する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。

match ipv6 hop-limit

no match ipv6 hop-limit

構文の説明

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

ユーザ定義のフロー レコードのキー フィールドとして IPv6 ホップ リミットを使用する設定は、デフォルトでイネーブルになっていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードにキー フィールドが含まれていない場合は、フロー モニタで使用することができません。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、キー フィールドとしてフロー パケットのホップ リミットを設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 hop-limit
```

関連トピック

flow record, （92 ページ）

match ipv6 source address

IPv6 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 source address** コマンドを使用します。IPv6 送信元アドレスをフロー レコードのキーフィールドとして使用するの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。

match ipv6 source address

no match ipv6 source 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

IPv6 送信元アドレスはキー フィールドとして設定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードにキー フィールドが含まれていない場合は、フロー モニタで使用することができません。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドで指定します。

このコマンドをデフォルト設定に戻すには、**no match ipv6 source address** または **default match ipv6 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、IPv6 送信元アドレスをキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 source address
```

関連トピック

flow record, （92 ページ）

match transport

フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match transport** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを使用する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。

match transport {**destination-port**| **icmp ipv4**| **icmp ipv6**| **igmp type**| **source-port**}

no match transport {**destination-port**| **icmp ipv4**| **icmp ipv6**| **igmp type**| **source-port**}

構文の説明

destination-port	キー フィールドとしてトランスポート宛先ポートを設定します。
icmp ipv4	ICMP IPv4 のタイプ フィールドとコード フィールドをキー フィールドとして設定します。詳細については、 match transport icmp ipv4, （112 ページ）を参照してください。
icmp ipv6	ICMP IPv6 のタイプ フィールドとコード フィールドをキー フィールドとして設定します。詳細については、match transport icmp ipv6, （113 ページ）を参照してください。

igmp type	システム稼働時間に基づくタイム スタンプをキー フィールドとして設定します。
source-port	キー フィールドとしてトランスポート送信元ポートを設定します。

コマンド デフォルト

トランスポート フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キーフィールドは、match コマンドを使用して定義されます。

次の例では、宛先ポートをキー フィールドとして設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport destination-port
```

次の例では、送信元ポートをキー フィールドとして設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport source-port
```

関連トピック

flow record, （92 ページ）

match transport icmp ipv4

ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv4** コマンドを使用します。ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するの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。

match transport icmp ipv4 {**code**| **type**}

no match transport icmp ipv4 {**code**| **type**}

構文の説明

code	ICMP IPv4 コードをキー フィールドとして設定します。
type	ICMP IPv4 タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv4 のタイプ フィールドとコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キー フィールドは、match コマンドを使用して定義されます。

次に、ICMP IPv4 コード フィールドをキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 code
```

次に、ICMP IPv4 タイプ フィールドをキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 type
```

関連トピック

flow record, （92 ページ）

match transport icmp ipv6

ICMP IPv6 タイプ フィールドおよびコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv6** コマンドを使用します。ICMP IPv6 タイプ フィールドおよびコード フィールドをフロー レコードの

キー フィールドとして使用する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。

match transport icmp ipv6 {**code**| **type**}

no match transport icmp ipv6 {**code**| **type**}

構文の説明

code	IPv6 ICMP コードをキー フィールドとして設定します。
type	IPv6 ICMP タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv6 タイプ フィールドおよびコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。各フローには、各キー フィールドに 1 組の一意の値が設定されているため、このキー フィールドによって各フローが区別されます。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、IPv6 ICMP コード フィールドをキー フィールドとして設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 code
```

次の例では、IPv6 ICMP タイプ フィールドをキー フィールドとして設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 type
```

関連トピック

flow record, （92 ページ）

mode random 1 out-of

ランダム サンプリングを有効にし、Flexible NetFlow サンプラーのパケット間隔を指定するには、サンプラー コンフィギュレーション モードで **mode random 1 out-of** コマンドを使用します。Flexible NetFlow サンプラーのパケット間隔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。

mode random 1 out-of *window-size*

no mode

構文の説明

window-size	パケットを選択するウィンドウ サイズを指定します。指定できる範囲は 2 ～ 1024 です。

コマンド デフォルト

サンプラーのモードとパケット間隔は設定されていません。

コマンド モード

サンプラー 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**deterministic** キーワードが削除されました。

使用上のガイドライン

では、計 4 つの固有のサンプラーがサポートされています。パケットは、トラフィック パターンのバイアスを除外し、モニタリングを回避するためのユーザによる試行を無効にする方法で選択されます。

（注） **deterministic** 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。

次の例では、ウィンドウ サイズ 1000 でランダム サンプリングをイネーブルにします。

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)# mode random 1 out-of 1000
```

関連トピック

debug sampler, （84 ページ）
show sampler, （130 ページ）

オプション

Flexible NetFlow のフローエクスポータのオプションのデータ パラメータを設定するには、フローエクスポータ コンフィギュレーション モードで **option** コマンドを使用します。フローエクスポータのオプションのデータ 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。

option {**exporter-stats**| **interface-table**| **sampler-table**} [**timeout** *seconds*]

no option {**exporter-stats**| **interface-table**| **sampler-table**}

構文の説明

exporter-stats	フロー エクスポータの統計情報オプションを設定します。
interface-table	フロー エクスポータのインターフェイス テーブル オプションを設定します。
sampler-table	フロー エクスポータのエクスポート サンプラー テーブル オプションを設定します。
timeout*seconds*	（任意）フローエクスポータのオプションの再送時間を秒単位で設定します。指定できる範囲は 1 ～ 86400 です。デフォルトは 600 です。

コマンド デフォルト

タイムアウトは 600 秒です。他のすべてのオプション データ パラメータは設定されていません。

コマンド モード

フロー エクスポータ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**application-table** および **usermac-table** キーワードが追加されました。

使用上のガイドライン

option exporter-stats コマンドを実行すると、レコード数、バイト数、送信されたパケット数など、エクスポータの統計情報が定期的に送信されます。このコマンドを使用して、コレクタは受信するエクスポート レコードのパケット損失を見積もります。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

option interface-table コマンドを実行すると、オプション テーブルが定期的に送信されます。このオプション テーブルを使用して、コレクタはフロー レコードに記録されている SNMP インターフェイス インデックスを各インターフェイス名にマッピングします。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

option sampler-table コマンドを実行すると、オプション テーブルが定期的に送信されます。このオプション テーブルには、各サンプラーの設定の詳細が含まれており、これを使用して、コレクタは任意のフロー レコードに記録されているサンプラー ID を、フローの統計情報のスケール アップに使用可能な設定にマッピングします。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

このコマンドをデフォルト設定に戻すには、**no option** または **default option** フロー エクスポータ コンフィギュレーション コマンドを使用します。

次の例では、サンプラー オプション テーブルの定期的な送信をイネーブルにして、コレクタでサンプラー ID をサンプラーのタイプとレートにマッピングする方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

次の例では、レコード数、バイト数、送信されたパケット数など、エクスポータの統計情報の定期的な送信をイネーブルする方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

次の例では、オプション テーブルの定期的な送信をイネーブルにし、そのオプション テーブルをコレクタで使用して、フロー レコードに記録されている SNMP インターフェイス インデックスをインターフェイス名にマッピングする方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
```

関連トピック

フロー エクスポータ，（90 ページ）

record

Flexible NetFlow フロー モニタのフロー レコードを追加するには、フロー モニタ コンフィギュレーション モードで **record** コマンドを使用します。Flexible NetFlow フロー モニタのフロー レコードを削除するには、このコマンドの **no** 形式を使用します。

record *record-name*

no record

構文の説明

record-name	事前に設定したユーザ定義のフロー レコードの名前。

コマンド デフォルト

フロー レコードは設定されていません。

コマンド モード

フロー モニタ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フローモニタごとに、キャッシュエントリの内容およびレイアウトを定義するレコードが必要です。フローモニタがさまざまな事前定義済みレコード フォーマットの 1 つを使用することも、上級ユーザが独自のレコード フォーマットを作成することもできます。

（注） フローモニタで **record** コマンドのパラメータを変更する前に、**noipflowmonitor** コマンドを使用して、すべてのインターフェイスから適用済みのフローモニタを削除する必要があります。

次の例では、FLOW-RECORD-1 を使用するようにフロー モニタを設定します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record FLOW-RECORD-1
```

関連トピック

フロー モニタ，（91 ページ）

sampler

Flexible NetFlow フロー サンプラーを作成するか、または既存の Flexible NetFlow フロー サンプラーを変更し、Flexible NetFlow サンプラー 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、**sampler** コマンドを使用します。サンプラーを削除するには、このコマンドの **no** 形式を使用します。

sampler *sampler-name*

no sampler *sampler-name*

構文の説明

sampler-name	作成または変更するフロー サンプラーの名前。

コマンド デフォルト

Flexible NetFlow フロー サンプラーは設定されません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー サンプラーは分析されるパケット数を制限することで、トラフィックをモニタするために Flexible NetFlow によってネットワーク デバイスで生じる負荷を軽減するために使用されます。2 ～ 1024 パケットの範囲から 1 パケットの割合でサンプリング レートを設定します。フロー サンプラーは、サンプリングされた Flexible NetFlow を実装するためにフローモニタとともにインターフェイスに適用されます。

フローサンプリングをイネーブルにするには、トラフィック分析に使用して、フローモニタに割り当てるレコードを設定します。インターフェイスにサンプラーを含むフロー モニタを適用すると、サンプリングされたパケットはサンプラーによって指定されたレートで分析され、フロー モニタに対応するフロー レコードと比較されます。分析されるパケットがフロー レコードによって指定された条件を満たす場合、フロー モニタ キャッシュに追加されます。

次に、フロー サンプラーの名前 SAMPLER-1 を作成する例を示します。

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)#
```

関連トピック

debug sampler, （84 ページ）
mode
show sampler, （130 ページ）

show flow exporter

フロー エクスポータのステータスと統計情報を表示するには、特権 EXEC モードで **show flow exporter** コマンドを使用します。

show flow exporter [**broker** [**detail**| **picture**]| **export-ids netflow-v9**| [**name**] *exporter-name* [**statistics**| **templates**]| **statistics**| **templates**]

構文の説明

broker	（任意）Flexible NetFlow フローエクスポータのブローカのステータスに関する情報を表示します。
detail	（任意）フローエクスポータのブローカに関する詳細な情報を表示します。
picture	（任意）ブローカ状態の画像を表示します。
export-ids netflow-v9	（任意）エクスポート可能な NetFlow バージョン 9 エクスポート フィールドとその ID を表示します。
name	（任意）フロー エクスポータの名前を指定します。
exporter-name	（任意）前に設定されたフロー エクスポータの名前。
statistics	（任意）すべてのフロー エクスポータまたは指定されたフロー エクスポータの統計情報を表示します。
templates	（任意）すべてのフロー エクスポータまたは指定されたフロー エクスポータのテンプレート情報を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、デバイスで設定されているすべてのフロー エクスポータのステータスと統計情報を表示する例を示します。

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:              Exports to the datacenter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:      192.168.0.2
    Transport Protocol:     UDP
    Destination Port:       9995
    Source Port:            55864
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

次の表で、こ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。

表 *6*：*show flow exporter* のフィールドの説明

フィールド	説明
Flow Exporter	設定したフロー エクスポータの名前。
Description	エクスポータに設定した説明、またはユーザ定義のデフォルトの説明。
Transport Configuration	このエクスポータのトランスポート設定フィールド。
Destination IP address	宛先ホストの IP アドレス。
Source IP address	エクスポートされたパケットで使用される送信元 IP アドレス。
Transport Protocol	エクスポートされたパケットで使用されるトランスポート層プロトコル。
Destination Port	エクスポートされたパケットが送信される宛先 UDP ポート。
Source Port	エクスポートされたパケットが送信される送信元 UDP ポート。
DSCP	Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値。
TTL	存続可能時間値。

フィールド	説明
Output Features	**output-features** コマンドが使用されたかどうかを指定します。このコマンドが使用されると、Flexible NetFlow エクスポート パケット上で出力機能が実行されます。

次に、デバイスで設定されているすべてのフロー エクスポータのステータスと統計情報を表示する例を示します。

```
Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:         0                     (0 bytes)
```

関連トピック

clear flow exporter, （71 ページ）

debug flow exporter, （81 ページ）

フロー エクスポータ, （90 ページ）

show flow interface

インターフェイスの Flexible NetFlow 設定およびステータスを表示するには、特権 EXEC モードで **showflowinterface** コマンドを使用します。

show flow interface [*type number*]

構文の説明

type	（任意）Flexible NetFlow アカウンティング設定情報を表示するインターフェイスのタイプ。
number	（任意）Flexible NetFlow アカウンティング設定情報を表示するインターフェイスの番号。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、イーサネット インターフェイス 0/0 と 0/1 の Flexible NetFlow アカウンティング設定を表示する例を示します。

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
        monitor:          FLOW-MONITOR-1
        direction:        Output
        traffic(ip):      on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
        monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      sampler SAMPLER-2#
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *7* : *show flow interface* のフィールドの説明

フィールド	説明
Interface	情報が適用されるインターフェイス。
monitor	インターフェイス上に設定されているフローモニタの名前
direction:	フロー モニタによってモニタされているトラフィックの方向。 次の値が可能です。 • Input：インターフェイスが受信しているトラフィック。 • Output：インターフェイスが送信しているトラフィック。
traffic(ip)	フロー モニタが通常モードとサンプラー モードのどちらであるかを示します。 次の値が可能です。 • on：通常モード。 • sampler：サンプラー モード（サンプラーの名前も表示されます）。

関連トピック

show flow monitor, （124 ページ）

show flow monitor

Flexible NetFlow フロー モニタのステータスと統計情報を表示するには、特権 EXEC モードで **showflowmonitor** コマンドを使用します。

show flow monitor [**broker** [**detail**| **picture**]| [**name**] *monitor-name* [**cache** [**format** {**csv**| **record**| **table**}]]| **provisioning**| **statistics**]

構文の説明

broker	（任意）フロー モニタのブローカの状態に関する情報を表示します。
detail	（任意）フロー モニタのブローカに関する詳細情報を表示します。
picture	（任意）ブローカ状態の画像を表示します。
name	（任意）フロー モニタの名前を指定します。
monitor-name	（任意）事前に設定されたフロー モニタの名前。
cache	（任意）フロー モニタのキャッシュの内容を表示します。
format	（任意）ディスプレイ出力のフォーマット オプションのいずれかを使用することを指定します。
csv	（任意）フローモニタのキャッシュの内容をカンマ区切り値（CSV）形式で表示します。
record	（任意）フロー モニタのキャッシュの内容をレコード形式で表示します。
table	（任意）フロー モニタのキャッシュの内容を表形式で表示します。
provisioning	（任意）フロー モニタのプロビジョニング情報を表示します。
statistics	（任意）フロー モニタの統計情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

cache キーワードでは、デフォルトでレコード形式が使用されます。

showflowmonitor*monitor-name***cache** コマンドのディスプレイ出力に含まれる大文字のフィールド名は、フローを識別するために Flexible NetFlow で使用されるキー フィールドです。**showflowmonitor***monitor-name***cache** コマンドのディスプレイ出力に含まれる小文字のフィールド名は、Flexible NetFlow がキャッシュの追加データとして値を収集する非キー フィールドです。

次の例では、フロー モニタのステータスを表示します。

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *8*：*show flow monitor monitor-name* フィールドの説明

フィールド	説明
Flow Monitor	設定したフロー モニタの名前。
説明	モニタに設定した説明、またはユーザ定義のデフォルトの説明。
Flow Record	フロー モニタに割り当てられたフロー レコード。
Flow Exporter	フローモニタに割り当てられたエクスポータ。
Cache	フロー モニタのキャッシュに関する情報。
Type	フロー モニタのキャッシュ タイプ。この値は常に normal となります。これが唯一サポートされているキャッシュ タイプです。

フィールド	説明
Status	フロー モニタのキャッシュのステータス。 次の値が可能です。 • allocated：キャッシュが割り当てられています。 • being deleted：キャッシュが削除されています。 • not allocated：キャッシュが割り当てられていません。
Size	現在のキャッシュ サイズ。
Inactive Timeout	非アクティブ タイムアウトの現在の値（秒単位）。
Active Timeout	アクティブ タイムアウトの現在の値（秒単位）。

次の例では、FLOW-MONITOR-1という名前のフローモニタのステータス、統計情報、およびデータを表示します。

```
Device# show flow monitor FLOW-MONITOR-1 cache
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001:DB8::1
IPV6 DESTINATION ADDRESS:                2001:DB8:1::1
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *9* : ***show flow monitor monitor-name cache*** フィールドの説明

フィールド	説明
Cache type	フロー モニタのキャッシュ タイプ。この値は常に normal となります。これが唯一サポートされているキャッシュ タイプです。
Cache Size	キャッシュ内のエントリ数。
Current entries	キャッシュ内の使用中のエントリ数。
Flows added	キャッシュの作成後にキャッシュに追加されたフロー
Flows aged	キャッシュの作成後に期限切れになったフロー
Active timeout	アクティブ タイムアウトの現在の値（秒単位）。
Inactive timeout	非アクティブ タイムアウトの現在の値（秒単位）。
DATALINK MAC SOURCE ADDRESS INPUT	入力パケットの MAC 送信元アドレス。
DATALINK MAC DESTINATION ADDRESS INPUT	入力パケットの MAC 宛先アドレス。
IPV6 SOURCE ADDRESS	IPv6 送信元アドレスです。
IPV6 DESTINATION ADDRESS	IPv6 宛先アドレス。
TRNS SOURCE PORT	トランスポート プロトコルの送信元ポート。
TRNS DESTINATION PORT	トランスポート プロトコルの宛先ポート。
IP VERSION	IP バージョン。
IP PROTOCOL	プロトコル番号。
IP TOS	IP タイプ オブ サービス（ToS）の値。
IP TTL	IP 存続可能時間（TTL）の値。
tcp flags	TCP フラグの値。
counter bytes	カウントされたバイト数。

フィールド	説明
counter packets	カウントされたパケット数。

次の例では、FLOW-MONITOR-1という名前のフローモニタのステータス、統計情報、およびデータを表形式で表示します。

```
Device# show flow monitor FLOW-MONITOR-1 cache format table
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2

DATALINK MAC SRC ADDR INPUT  DATALINK MAC DST ADDR INPUT  IPV6 SRC ADDR  IPV6 DST ADDR
TRNS SRC PORT  TRNS DST PORT  IP VERSION  IP PROT  IP TOS  IP TTL  tcp flags  bytes long
pkts long
===========================  ===========================  =============  =============
=============  =============  ==========  =======  ======  ======  =========  ==========
=========
0000.0000.1000               6400.F125.59E6               2001:DB8::1    2001:DB8:1::1
        1111           2222           6        6  0x05        11  0x20        132059538
1158417
```

次の例では、FLOW-MONITOR-IPv6という名前のフロー モニタ（キャッシュにIPv6データを格納）のステータス、統計情報、およびデータをレコード形式で表示します。

```
Device# show flow monitor name FLOW-MONITOR-IPv6 cache format record
  Cache type:                                 Normal (Platform cache)
  Cache size:                                Unknown
  Current entries:                                 1

  Flows added:                                     3
  Flows aged:                                      2
    - Active timeout      (   300 secs)            2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001::2
IPV6 DESTINATION ADDRESS:                2002::2
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

次の例では、フロー モニタのステータスと統計情報を表示します。

```
Device# show flow monitor FLOW-MONITOR-1 statistics
  Cache type:                                 Normal (Platform cache)
  Cache size:                                Unknown
  Current entries:                                 1

  Flows added:                                     3
  Flows aged:                                      2
    - Active timeout      (   300 secs)            2
```

関連トピック

clear flow monitor, （72 ページ）

debug flow monitor, （82 ページ）

show flow record

Flexible NetFlow フロー レコードのステータスと統計情報を表示するには、特権 EXEC モードで **show flow record** コマンドを使用します。

show flow record [**broker** [**detail**| **picture**]| [**name**]*record-name*]

構文の説明

broker	（任意）Flexible NetFlow フロー レコードのブローカのステータスに関する情報を表示します。
detail	（任意）フロー レコードのブローカに関する詳細な情報を表示します。
picture	（任意）ブローカ状態の画像を表示します。
name	（任意）フロー レコードの名前を指定します。
record-name	（任意）前に設定されたユーザ定義のフロー レコードの名前。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、FLOW-RECORD-1 のステータスおよび統計情報を表示する例を示します。

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:        User defined
  No. of users:       0
  Total field space:  24 bytes
  Fields:
```

```
match ipv6 destination address
match transport source-port
collect interface input
```

関連トピック

record, （117 ページ）

show sampler

Flexible NetFlow サンプラーのステータスと統計情報を表示するには、特権 EXEC モードで **show sampler** コマンドを使用します。

show sampler [**broker** [**detail**| **picture**]| [**name**]*sampler-name*]

構文の説明

broker	（任意）Flexible NetFlow サンプラーのブローカのステータスに関する情報を表示します。
detail	（任意）サンプラーのブローカに関する詳細な情報を表示します。
picture	（任意）ブローカ状態の画像を表示します。
name	（任意）サンプラーの名前を指定します。
sampler-name	（任意）前に設定されたサンプラーの名前。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、設定されたフロー サンプラーすべてのステータスと統計情報を表示する例を示します。

```
Device# show sampler
Sampler SAMPLER-1:
  ID:             2083940135
  export ID:      0
```

```
  Description:    User defined
  Type:           Invalid (not in use)
  Rate:           1 out of 32
  Samples:        0
  Requests:       0
  Users (0):

Sampler SAMPLER-2:
  ID:             3800923489
  export ID:      1
  Description:    User defined
  Type:           random
  Rate:           1 out of 100
  Samples:        1
  Requests:       124
  Users (1):
    flow monitor FLOW-MONITOR-1 (datalink,vlan1)  0 out of 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *10*：*show sampler* のフィールドの説明

フィールド	説明
ID	フロー サンプラーの ID 番号。
Export ID	フロー サンプラーのエクスポートの ID。
Description	フローサンプラーに設定した説明、またはユーザ定義のデフォルトの説明。
Type	フローサンプラーに設定したサンプリング モード。
Rate	フロー サンプラーに設定したウィンドウ サイズ（パケットの選択用）。指定できる範囲は 2 ～ 32768 です。
Samples	フローサンプラーを設定してから、またはデバイスを再起動してからサンプリングされたパケットの数。この数は、トラフィックのサンプリングが必要かどうかを決定するためにサンプラーが呼び出されたときに肯定応答を受信した回数と同じです。この表の Requests フィールドの説明を参照してください。
Requests	トラフィックのサンプリングが必要かどうかを決定するためにサンプラーが呼び出された回数。
Users	フローサンプラーが設定されるインターフェイス。

関連トピック

debug sampler, （84 ページ）
sampler, （118 ページ）

source

Flexible NetFlow フロー エクスポータから送信されるすべてのパケットの送信元 IP アドレスのインターフェイスを設定するには、フロー エクスポータ コンフィギュレーション モードで **source** コマンドを使用します。Flexible NetFlow フローエクスポータから送信されるすべてのパケットの送信元 IP アドレスのインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

source *interface-type interface-number*

no source

構文の説明

interface-type	Flexible NetFlow フローエクスポータから送信されるパケットの送信元 IP アドレス向けに使用する IP アドレスのインターフェイスのタイプ。
interface-number	Flexible NetFlow フローエクスポータから送信されるパケットの送信元 IP アドレス向けに使用する IP アドレスのインターフェイス番号。

コマンド デフォルト

Flexible NetFlow データグラムを送信するインターフェイスの IP アドレスが、送信元 IP アドレスとして使用されます。

コマンド モード

フロー エクスポータ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

Flexible NetFlow が送信するデータグラムに一貫した送信元 IP アドレスを使用することの利点として、以下が含まれます。

- Flexible NetFlow によりエクスポートされるデータグラムの送信元 IP アドレスは、Flexible NetFlow データがどちらのデバイスから到着するかを判断するために、宛先システムによって使用されます。デバイスから宛先システムに Flexible NetFlow データグラムを送信するのに使用できるパスがネットワークに複数あり、送信元 IP アドレスを取得する送信元インターフェイスが指定されていない場合、デバイスはデータグラムが送信されるインターフェイスの IP アドレスを、データグラムの送信元 IP アドレスとして使用します。この場合、宛先システムは同じデバイスから送信元 IP アドレスが異なる Flexible NetFlow データグラムを受信する場合があります。宛先システムが、異なる送信元 IP アドレスを持つ同じデバイスから Flexible NetFlow データグラムを受信すると、宛先システムは異なるデバイスから送信されたものとして Flexible NetFlow データグラムを処理します。宛先システムが Flexible NetFlow データグラムを異なるデバイスから送信されたものとして処理しないようにするには、宛先システムがデバイスですべての可能な送信元 IP アドレスから受信する Flexible NetFlow データグラムを単一の Flexible NetFlow フローに集約するように、宛先システムを設定する必要があります。
- データグラムを宛先システムに送信するために使用できる複数のインターフェイスがデバイスにあり、**source** コマンドを設定していない場合、Flexible NetFlow トラフィックを許可するために作成するアクセス リストに、各インターフェイスの IP アドレスのエントリを追加する必要があります。既知の送信元からの Flexible NetFlow トラフィックを許可し、不明な送信元からはブロックするためにアクセス リストを作成および維持することは、Flexible NetFlow トラフィックをエクスポートするデバイスごとに単一の IP アドレスに Flexible NetFlow データグラムの送信元 IP アドレスを制限すると、より簡単に行えるようになります。

注意 **送信元**インターフェイスとして設定するインターフェイスには、設定された IP アドレスが必須であり、アップされている必要があります。

ヒント **source** コマンドで設定したインターフェイス上で一時的な停止が発生した場合、Flexible NetFlow エクスポータは、データグラムが送信されるインターフェイスの IP アドレスをデータグラムの送信元 IP アドレスとして使用するデフォルトの動作に戻ります。この問題を回避するには、ループバック インターフェイスを送信元インターフェイスとして使用します。これは、ループバック インターフェイスが物理インターフェイスで発生する可能性のある一時的な停止の影響を受けないためです。

このコマンドをデフォルト設定に戻すには、**no source** または **default source** フロー エクスポータ コンフィギュレーション コマンドを使用します。

次に、NetFlow トラフィックの送信元インターフェイスとして、ループバック インターフェイスを使用するように Flexible NetFlow を設定する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# source loopback 0
```

関連トピック

フロー エクスポータ，（90 ページ）

template data timeout

フロー エクスポータ テンプレート データの再送信のタイムアウト期間を指定するには、フロー エクスポータ コンフィギュレーション モードで **template data timeout** コマンドを使用します。フロー エクスポータの再送信のタイムアウトを削除するには、このコマンドの **no** 形式を使用します。

template data timeout *seconds*

no template data timeout *seconds*

構文の説明

seconds	秒単位のタイムアウト値です。指定できる範囲は1～86400です。デフォルトは 600 です。

コマンド デフォルト

デフォルトのフロー エクスポータ テンプレート再送信のタイムアウトは、600 秒です。

コマンド モード

フロー エクスポータ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

フロー エクスポータのテンプレート データには、エクスポートされるデータ レコードが記述されています。対応するテンプレートなしでデータ レコードをデコードすることはできません。**template data timeout** コマンドを使用して、これらのテンプレートをエクスポートする頻度を制御します。

このコマンドをデフォルト設定に戻すには、**no template data timeout** または **default template data timeout** フロー レコード エクスポータ コマンドを使用します。

次の例では、1000 秒というタイムアウトに基づいてテンプレートの再送信を設定します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# template data timeout 1000
```

関連トピック

フロー エクスポータ, （90 ページ）

transport

Flexible NetFlow のフロー エクスポータのトランスポート プロトコルを設定するには、フロー エクスポータ コンフィギュレーション モードで **transport** コマンドを使用します。フロー エクスポータのトランスポート プロトコルを削除するには、このコマンドの **no** 形式を使用します。

transport udp *udp-port*

no transport udp *udp-port*

構文の説明

udp *udp-port*	トランスポート プロトコルとして User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を指定し、UDP ポート番号を指定します。

コマンド デフォルト

フロー エクスポータでは、UDP をポート 9995 で使用します。

コマンド モード

フロー エクスポータ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、**no transport** または **default transport flow exporter** コンフィギュレーション コマンドを使用します。

次に、トランスポート プロトコルとして UDP を設定し、UDP ポート番号を 250 に設定する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# transport udp 250
```

関連トピック

フロー エクスポータ, （90 ページ）

ttl

存続可能時間（TTL）を設定するには、フロー エクスポータ コンフィギュレーション モードで **ttl** コマンドを使用します。TTL 値を削除するには、このコマンドの **no** 形式を使用します。

ttl *ttl*

no ttl *ttl*

構文の説明

ttl	エクスポートされたデータグラムの存続可能時間（TTL）値。指定できる範囲は 1 ～ 255 です。デフォルトは 255 です。

コマンド デフォルト

フロー エクスポータでは TTL 値 255 が使用されています。

コマンド モード

フロー エクスポータ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、 **no ttl** または **default ttl** フロー エクスポータ コンフィギュレーション コマンドを使用します。

次に、TTL 値 15 を指定する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# ttl 15
```

関連トピック

フロー エクスポータ, （90 ページ）

第 IV 部

インターフェイスおよびハードウェア コンポーネント

- インターフェイスおよびハードウェア コマンド，139 ページ

第 5 章

インターフェイスおよびハードウェア コマンド

- client vlan, 141 ページ
- debug ilpower, 142 ページ
- debug interface, 144 ページ
- debug lldp packets, 145 ページ
- debug nmsp, 146 ページ
- debug platform poe, 147 ページ
- duplex, 148 ページ
- errdisable detect cause, 150 ページ
- errdisable recovery cause, 152 ページ
- errdisable recovery interval, 155 ページ
- interface, 156 ページ
- interface range, 157 ページ
- ip mtu, 159 ページ
- ipv6 mtu, 160 ページ
- lldp（インターフェイス コンフィギュレーション）, 161 ページ
- logging event power-inline-status, 163 ページ
- mdix auto, 164 ページ
- mode（電源スタックの設定）, 165 ページ
- network-policy, 167 ページ
- network-policy profile（グローバル コンフィギュレーション）, 168 ページ

- nmsp attachment suppress, 169 ページ
- power efficient-ethernet auto, 170 ページ
- power-priority, 171 ページ
- power inline, 173 ページ
- power inline police, 177 ページ
- 電源装置, 179 ページ
- show CAPWAP summary, 181 ページ
- show controllers cpu-interface, 182 ページ
- show controllers ethernet-controller, 183 ページ
- show controllers utilization, 194 ページ
- show eee, 195 ページ
- show env, 199 ページ
- show errdisable detect, 202 ページ
- show errdisable recovery, 204 ページ
- show interfaces, 205 ページ
- show interfaces counters, 209 ページ
- show interfaces switchport, 212 ページ
- show interfaces transceiver, 214 ページ
- show memory platform, 217 ページ
- show module, 219 ページ
- show mgmt-infra trace messages ilpower, 220 ページ
- show mgmt-infra trace messages ilpower-ha, 221 ページ
- show mgmt-infra trace messages platform-mgr-poe, 222 ページ
- show network-policy profile, 223 ページ
- show platform CAPWAP summary, 224 ページ
- show platform forward, 224 ページ
- show platform hardware fed switch forward, 226 ページ
- show platform resources, 229 ページ
- show platform software ilpower, 229 ページ
- show platform software process list, 231 ページ
- show platform software process slot switch, 233 ページ

- show platform software status control-processor, 235 ページ
- show processes cpu platform monitor, 237 ページ
- show processes memory platform, 239 ページ
- show power inline, 242 ページ
- show stack-power, 248 ページ
- show system mtu, 250 ページ
- show tech-support, 251 ページ
- show wireless interface summary, 253 ページ
- speed, 254 ページ
- stack-power , 256 ページ
- switchport block, 257 ページ
- system mtu, 259 ページ
- test mcu read-register, 260 ページ
- voice-signaling vlan（ネットワークポリシー コンフィギュレーション）, 262 ページ
- voice vlan（ネットワークポリシー コンフィギュレーション）, 263 ページ
- wireless ap-manager interface, 265 ページ
- wireless exclusionlist, 266 ページ
- wireless linktest, 267 ページ
- wireless management interface, 268 ページ
- wireless peer-blocking forward-upstream, 268 ページ

client vlan

WLAN インターフェイスまたはインターフェイス グループを設定するには、**clientvlan** コマンドを使用します。WLAN インターフェイ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。

client vlan *interface-id-name-or-group-name*

no client vlan

構文の説明

interface-id-name-or-group-name	インターフェイス ID、名前、または VLAN グループ名。インターフェイス ID は、複数桁で指定することもできます。

コマンド デフォルト

WLAN の設定インターフェイスが設定されています。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント VLAN をイネーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client vlan client-vlan1
Device(config-wlan)# end
```

次に、WLAN 上のクライアント VLAN をディセーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no client vlan
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

debug ilpower

電源コントローラおよびPower over Ethernet（PoE）システムのデバッグをイネーブルにするには、特権 EXEC モードで **debug ilpower** コマンドを使用します。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 ilpower {**cdp**| **controller**| **event**| **ha**| **ipc**| **police**| **port**| **powerman**| **registries**| **scp**| **sense**| **upoe**}

no debug ilpower {**cdp**| **controller**| **event**| **ha**| **ipc**| **police**| **port**| **powerman**| **registries**| **scp**| **sense**| **upoe**}

構文の説明

cdp	PoE Cisco Discovery Protocol（CDP）デバッグ メッセージを表示します。
controller	PoE コントローラ デバッグ メッセージを表示します。
event	PoE イベント デバッグ メッセージを表示します。
ha	PoE ハイ アベイラビリティ メッセージを表示します。

ipc	PoE Inter-Process Communication（IPC）デバッグ メッセージを表示します。
police	PoE police デバッグ メッセージを表示します。
port	PoE ポート マネージャ デバッグ メッセージを表示します。
powerman	PoE 電力管理デバッグ メッセージを表示します。
registries	PoE レジストリ デバッグ メッセージを表示します。
scp	PoE SCP デバッグ メッセージを表示します。
sense	PoE sense デバッグ メッセージを表示します。
upoe	Cisco UPOE デバッグ メッセージを表示します。

コマンド 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**upoe** キーワードが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応スイッチだけでサポートされています。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session***switch-number* EXEC コマンドを使用して、active switch からのセッションを開始できます。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

debug interface

インターフェイス関連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には、このコマンドの **no** 形式を使用します。

debug interface {*interface-id*| **counters** {**exceptions**| **protocol memory**}| **states**}

no debug interface {*interface-id*| **counters** {**exceptions**| **protocol memory**}| **states**}

構文の説明

interface-id	物理インターフェイスの ID。タイプ スイッチ番号/モジュール番号/ポート（例：gigabitethernet 1/0/2）によって識別される指定された物理ポートのデバッグ メッセージを表示します。
counters	カウンタ デバッグ情報を表示します。
exceptions	インターフェイス パケットおよびデータ レート統計情報の計算中に回復可能な例外条件が発生したときにデバッグ メッセージを表示します。
protocol memory	プロトコル カウンタのメモリ操作のデバッグ メッセージを表示します。
states	インターフェイスの状態が移行するときに中間のデバッグ メッセージを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session***switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

debug lldp packets

Link Layer Discovery Protocol（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には、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。

コマンド 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
Cisco IOS XE 3.2SE	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 lldp packets コマンドは、**no debug lldp packets** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session***switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。

debug nmsp

スイッチの Network Mobility Services Protocol（NMSP）のデバッグをイネーブルにするには、特権 EXEC モードで **debug nmsp** コマンドを使用します。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 nmsp {**all**| **connection**| **detail**| **error**| **event**| **message** {**rx**| **tx**}| **packet**} [**switch** *switch-number*]

no debug nmsp {**all**| **connection**| **detail**| **error**| **event**| **message** {**rx**| **tx**}| **packet**} [**switch** *switch-number*]

構文の説明

all	すべての NMSP デバッグ メッセージを表示します。
connection	NMSP 接続イベントのデバッグ メッセージを表示します。
detail	NMSP の詳細なデバッグ メッセージを表示します。
error	NMSP エラー メッセージのデバッグ情報を表示します。
event	NMSP イベントのデバッグ メッセージを表示します。
message	NMSP メッセージのデバッグ情報を表示します。
rx	NMSP 受信メッセージのデバッグ情報を表示します。
tx	NMSP 送信メッセージのデバッグ情報を表示します。
packet	NMSP パケット イベントのデバッグ メッセージを表示します。
switch *switch-number*	（任意）NMSP デバッグ情報を表示するスイッチ番号を指定します。

コマンド 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
Cisco IOS XE 3.2SE	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 nmsp コマンドは、**no debug nmsp** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session***switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

debug platform poe

Power over Ethernet（PoE）ポー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 poe** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug platform poe [**error**| **info**] [**switch** *switch-number*]

no debug platform poe [**error**| **info**] [**switch** *switch-number*]

構文の説明

error	（任意）PoE 関連エラーのデバッグ メッセージを表示します。
info	（任意）PoE 関連情報のデバッグ メッセージを表示します。
switch *switch-number*	（任意）スタック メンバを指定します。このキーワードは、スタック対応スイッチでのみサポートされています。

コマンド 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
Cisco IOS XE 3.2SE	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 platform poe コマンドは、**no debug platform poe** コマンドと同じです。

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。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 {**auto**| **full**| **half**}

構文の説明

auto	自動によるデュプレックス設定をイネーブルにします。接続されたデバイス モードにより、ポートが自動的に全二重モードか半二重モードで動作すべきかを判断します。
full	全二重モードをイネーブルにします。
half	半二重モードをイネーブルにします（10 または 100 Mb/s で動作するインターフェイスに限る）。1000 または 10,000 Mb/s で動作するインターフェイスに対して半二重モードを設定できません。

コマンド デフォルト

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。

10 ギガビット イーサネット ポートではデュプレックス モードを設定できません。常に **full** です。

二重オプションは、1000BASE-*x* または 10GBASE-*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。

コマンド モード

インターフェイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

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、**full** を指定するのと同じ効果があります。

（注） デュプレックス モードが **auto** で接続されている装置が半二重で動作している場合、半二重モードはギガビット イーサネット インターフェイスでサポートされます。ただし、これらのインターフェイスを半二重モードで動作するように設定することはできません。

特定のポートを全二重または半二重のいずれかに設定できます。このコマンドの適用可能性は、スイッチが接続されているデバイスによって異なります。

両方のラインの終端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエーションをサポートし、もう片方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定し、サポートされている側で **auto** の設定を使用してください。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にある装置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。

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

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# duplex full
```

関連トピック

show interfaces, （205 ページ）

errdisable detect cause

特定の原因またはすべての原因に対してerrdisable検出をイネーブルにするには、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 shutdown vlan**| **dhcp-rate-limit**| **dtp-flap**| **gbic-invalid**| **inline-power**| **l2ptguard**| **link-flap**| **loopback**| **pagp-flap**| **pppoe-ia-rate-limit** | **security-violation shutdown vlan**| **sfp-config-mismatch**}

no errdisable detect cause {**all**| **arp-inspection**| **bpduguard shutdown vlan**| **dhcp-rate-limit**| **dtp-flap**| **gbic-invalid**| **inline-power**| **l2ptguard**| **link-flap**| **loopback**| **pagp-flap**| **pppoe-ia-rate-limit** | **security-violation shutdown vlan**| **sfp-config-mismatch**}

構文の説明

all	すべての errdisable の原因に対して、エラー検出をイネーブルにします。
arp-inspection	ダイナミック 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。
bpduguard shutdown vlan	BPDU ガードで VLAN ごとに errdisable をイネーブルにします。
dhcp-rate-limit	Dynamic Host Configuration Protocol（DHCP）スヌーピング用のエラー検出をイネーブルにします。
dtp-flap	ダイナミック トランキング 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。
gbic-invalid	無効なギガビット インターフェイス コンバータ（GBIC）モジュール用のエラー検出をイネーブルにします。 （注） このエラーは、無効な Small Form-Factor Pluggable（SFP）モジュールを意味します。
inline-power	Power over Ethernet（PoE）の errdisable 原因に対して、エラー検出をイネーブルにします。 （注） このキーワードは、PoE ポートを備えたスイッチでのみサポートされています。
l2ptguard	レイヤ2プロトコル トンネルのerrdisable原因に対して、エラー検出をイネーブルにします。
link-flap	リンクステートのフラップに対して、エラー検出をイネーブルにします。
loopback	検出されたループバックに対して、エラー検出をイネーブルにします。

pagp-flap	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。
pppoe-ia-rate-limit	PPPoE 中継エージェントのレート制限 errdisable 原因に対して、エラー検出をイネーブルにします。
security-violation shutdown vlan	音声認識 IEEE 802.1x セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。

コマンド デフォルト

検出はすべての原因に対してイネーブルです。VLAN ごとの errdisable を除くすべての原因について、ポート全体をシャットダウンするように設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、dhcp-rate-limit など）は、errdisable ステートが発生した理由です。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステートとなり、リンクダウン ステートに類似した動作ステートとなります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。ブリッジ プロトコル データ ユニット（BPDU）ガード、音声認識 802.1x セキュリティ、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 のみをシャットダウンするようにスイッチを設定できます。

errdisable recovery グローバル コンフィギュレーション コマンドを入力して、原因の回復メカニズムを設定する場合は、すべての原因がタイムアウトになった時点で、インターフェイスは errdisable ステートから抜け出して、処理を再試行できるようになります。回復メカニズムを設定しない場合は、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、インターフェイスを手動で errdisable ステートから回復させる必要があります。

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。

次の例では、リンクフラップ errdisable 原因に対して errdisable 検出をイネーブルにする方法を示します。

```
Device(config)# errdisable detect cause link-flap
```

次のコマンドでは、VLAN ごとの errdisable ステートで BPDU ガードをグローバルに設定する方法を示します。

```
Device(config)# errdisable detect cause bpduguard shutdown vlan
```

次のコマンドでは、VLAN ごとの errdisable ステートで音声認識 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。

```
Device(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。

errdisable recovery cause

特定の原因から回復するように error-disabled メカニズム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** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

errdisable recovery cause {**all**| **arp-inspection**| **bpduguard**| **channel-misconfig**| **dhcp-rate-limit**| **dtp-flap**| **gbic-invalid**| **inline-power**| **l2ptguard**| **link-flap**| **loopback**| **mac-limit**| **pagp-flap**| **port-mode-failure**| **pppoe-ia-rate-limit**| **psecure-violation**| **security-violation**| **sfp-config-mismatch**| **storm-control**| **udld**| **vmps**}

no errdisable recovery cause {**all**| **arp-inspection**| **bpduguard**| **channel-misconfig**| **dhcp-rate-limit**| **dtp-flap**| **gbic-invalid**| **inline-power**| **l2ptguard**| **link-flap**| **loopback**| **mac-limit**| **pagp-flap**| **port-mode-failure**| **pppoe-ia-rate-limit**| **psecure-violation**| **security-violation**| **sfp-config-mismatch**| **storm-control**| **udld**| **vmps**}

構文の説明

all	すべての errdisable の原因から回復するタイマーをイネーブルにします。
arp-inspection	アドレス解決プロトコル（ARP）検査による errdisable ステートから回復するためのタイマーをイネーブルにします。
bpduguard	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。
channel-misconfig	EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
dhcp-rate-limit	DHCP スヌーピング errdisable ステートから回復するタイマーをイネーブルにします。

dtp-flap	ダイナミック トランキング 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。
gbic-invalid	ギガビット インターフェイス コンバータ（GBIC）モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。 （注） このエラーは無効な Small Form-Factor Pluggable（SFP）の errdisable ステートを意味します。
inline-power	Power over Ethernet（PoE）の errdisable ステートから回復するタイマーをイネーブルにします。 このキーワードは、PoE ポートを備えたスイッチでのみサポートされています。
l2ptguard	レイヤ 2 プロトコル トンネルによる errdisable ステートから回復するためのタイマーをイネーブルにします。
link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
mac-limit	MAC 制限 errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	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。
port-mode-failure	ポート モードの変更失敗の 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。
pppoe-ia-rate-limit	PPPoE IA レート制限 errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポート セキュリティ違反ディセーブル ステートから回復するタイマーをイネーブルにします。
security-violation	IEEE 802.1x 違反ディセーブル ステートから回復するタイマーをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。
storm-control	ストーム制御エラーから回復するタイマーをイネーブルにします。

udld	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。
vmps	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。

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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（all、BDPU ガードなど）は、errdisable ステートが発生した理由として定義されます。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステート（リンクダウン ステートに類似した動作ステート）となります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

原因の回復をイネーブルにしない場合、インターフェイスは、**shutdown** 及び **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 error-disabled ステートのままです。原因の回復をイネーブルにした場合、インターフェイスは errdisable ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

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、手動でインターフェイスを error-disabled ステートから回復させる必要があります。

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。

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。

```
Device(config)# errdisable recovery cause bpduguard
```

関連トピック

errdisable recovery interval, （155 ページ）
show errdisable recovery, （204 ページ）
show interfaces, （205 ページ）

errdisable recovery interval

error-disabled ステートから回復する時間を指定するには、グローバル コンフィギュレーション モードで **errdisable recovery 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。

errdisable recovery interval *timer-interval*

no errdisable recovery interval *timer-interval*

構文の説明

timer-interval	errdisable ステートから回復する時間。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。デフォルトの間隔は 300 秒です。

コマンド デフォルト

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

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。

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。

次の例では、タイマーを 500 秒に設定する方法を示します。

```
Device(config)# errdisable recovery interval 500
```

関連トピック

errdisable recovery cause, （152 ページ）

show errdisable recovery, （204 ページ）

show interfaces, （205 ページ）

interface

インターフェイスを設定するには、**interface** コマンドを使用します。

interface {**Auto-Template** *Auto-Template interface-number*| **Capwap** *Capwap interface-number* | **Gigabit Ethernet** *Gigabit Ethernet interface number*| **Group VI** *Group VI interface number* **Internal Interface** *Internal Interface number* **Loopback** *Loopback interface number* **Null** *Null interface* **Port-channel** *interface number***Port-channel** *interface number* **TenGigabit Ethernet** *interface number* **Tunnel** *interface number* **Vlan** *interface number*}

構文の説明

Auto-Template*Auto-template interface-number*	自動テンプレートインターフェイスを設定できます。値の範囲は 1 ～ 999 です。
Capwap*Capwap interface number*	CAPWAP トンネル インターフェイスを設定できます。値の範囲は 0 ～ 2147483647 です。
GigabitEthernet*Gigabit Ethernet interface number*	ギガビット イーサネット IEEE 802.3z インターフェイスを設定できます。値の範囲は 0 ～ 9 です。
Group VI *Group VI interface number*	内部インターフェイスを設定できます。値の範囲は 0 ～ 9 です。
Internal Interface Internal Interface	内部インターフェイスを設定できます。
Loopback*Loopback Interface number*	ループバック インターフェイスを設定できます。値の範囲は 0 ～ 2147483647 です。
Null*Null interface number*	ヌル インターフェイスを設定できます。値は 0 です。

Port-channel*interface number*	イーサネットチャネルインターフェイスを設定できます。値の範囲は 1 ～ 128 です。
TenGigabitEthernet*interface number*	10 ギガビット イーサネット インターフェイスを設定できます。値の範囲は 0 ～ 9 です。
Tunnel*interface number*	トンネル インターフェイスを設定できます。値の範囲は 0 ～ 2147483647 です。
Vlan*interface number*	スイッチの VLAN インターフェイスを設定できます。値の範囲は 0 ～ 4098 です。

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
Cisco IOS XE 3.2SE	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「no」形式を使用できません。

次に、インターフェイスを設定する例を示します。

```
Device# interface Tunnel 15
```

interface range

インターフェイス範囲を設定するには、**interfacerange** コマンドを使用します。

interface range {**Gigabit Ethernet** *interface-number*| **Loopback** *interface-number*| **Port Channel** *interface-number*| **TenGigabit Ethernet** *interface-number* **Tunnel** *interface-number* **Vlan** *interface-number* **Macro** *WORD*}

構文の説明

GigabitEthernet*interface-number*	ギガビット イーサネット IEEE 802.3z インターフェイスを設定します。値の範囲は 1 ～ 9 です。
Loopback*interface-number*	ループバック インターフェイスを設定します。値の範囲は 0 ～ 2147483647 です。
Port-Channel*interface-number*	インターフェイスの 10 ギガビット イーサネット チャネルを設定します。値の範囲は 1 ～ 128 です。
TenGigabit Ethernet*interface-number*	10 ギガビット イーサネット インターフェイスを設定します。値の範囲は 0 ～ 9 です。
Tunnel*interface-number*	トンネル インターフェイスを設定します。値の範囲は 0 ～ 2147483647 です。
VLAN*interface-number*	スイッチの VLAN インターフェイスを設定します。値の範囲は 1 ～ 4095 です。
Macro*WORD*	インターフェイスに対するキーワードを設定します。最大 32 文字までサポートされます。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、インターフェイス範囲を設定する例を示します。

```
Device(config)# interface range vlan 1
```

ip mtu

スイッチまたはスイッチ スタックのすべてのルーテッド ポートのルーテッド パケットの IP 最大伝送ユニット（MTU）サイズを設定するには、インターフェイス コンフィギュレーション モードで **ip mtu** コマンドを使用します。デフォルトの IP MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ip mtu *bytes*

no ip mtu *bytes*

構文の説明

bytes	MTU サイズ（バイト単位）。指定できる範囲は 68 からシステム MTU 値（バイト単位）までです。

コマンド デフォルト

すべてのスイッチインターフェイスで送受信されるフレームのデフォルト IP MTU サイズは、1500 バイトです。

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
Cisco IOS XE 3.2SE	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 値の上限は、スイッチまたはスイッチ スタックの設定に基づき、現在適用されているシステム MTU 値を参照します。MTU サイズの設定に関する詳細については、**system mtu** 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。

デフォルトの IP MTU 設定に戻すには、インターフェイスで **default ip mtu** コマンドまたは **no ip mtu** コマンドを適用できます。

show ip interface *interface-id* または **show interfaces** *interface-id* 特権 EXEC コマンドを入力して設定を確認できます。

次に、VLAN 200 の最大 IP パケット サイズを 1000 バイト に設定する例を示します。

```
Device(config)# interface vlan 200
Device(config-if)# ip mtu 1000
```

次に、VLAN 200 の最大 IP パケット サイズをデフォルト設定の 1500 バイト に設定する例を示します。

```
Device(config)# interface vlan 200
Device(config-if)# default ip mtu
```

次に、**show ip interface** *interface-id* コマンドの出力の一部を示します。インターフェイスの現在の IP MTU 設定が表示されます。

```
Device# show ip interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set

<output truncated>
```

ipv6 mtu

スイッチまたはスイッチ スタックのすべてのルーテッド ポートにルーテッド パケットの IPv6 最大伝送ユニット（MTU）サイズを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mtu** コマンドを使用します。デフォルトの IPv6 MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ipv6 mtu *bytes*

no ipv6 mtu *bytes*

構文の説明

bytes	MTU サイズ（バイト単位）。指定できる範囲は 1280 からシステム MTU 値（バイト単位）までです。

コマンド デフォルト

すべてのスイッチ インターフェイスで送受信されるフレームのデフォルト IPv6 MTU サイズは、1500 バイトです。

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
Cisco IOS XE 3.2SE	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 MTU 値の上限は、スイッチまたはスイッチ スタックの設定に基づき、現在適用されているシステム MTU 値を参照します。MTU サイズの設定に関する詳細については、**system mtu** 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。

デフォルトの IPv6 MTU 設定に戻すには、インターフェイスで **default ipv6 mtu** コマンドまたは **no ipv6 mtu** コマンドを適用できます。

show ipv6 interface*interface-id* または **show interface***interface-id* 特権 EXEC コマンドを入力して設定を確認できます。

次に、インターフェイスの最大 IPv6 パケット サイズを 2000 バイトに設定する例を示します。

```
Device(config)# interface gigabitethernet4/0/1
Device(config-if)# ipv6 mtu 2000
```

次に、インターフェイスの最大 IPv6 パケット サイズをデフォルト設定の 1500 バイトに設定する例を示します。

```
Device(config)# interface gigabitethernet4/0/1
Device(config-if)# default ipv6 mtu
```

次に、**show ipv6 interface***interface-id* コマンドの出力の一部を示します。インターフェイスの現在の IPv6 MTU 設定が表示されます。

```
Device# show ipv6 interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set

<output truncated>
```

lldp（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 Link Layer Discovery Protocol（LLDP）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 **lldp** コマンドを使用します。インターフェイスで LLDP 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。

lldp {**med-tlv-select** *tlv*| **receive**| **tlv-select power-management**| **transmit**}

no lldp {**med-tlv-select** *tlv*| **receive**| **tlv-select power-management**| **transmit**}

構文の説明

med-tlv-select	LLDP Media Endpoint Discovery（LLDP-MED）の Time Length Value（TLV）要素を送信するように選択します。
tlv	TLV 要素を特定するストリング。有効な値は次のとおりです。 • **inventory-management**：LLDP-MED インベントリ管理 TLV • **location**：LLDP-MED ロケーション TLV • **network-policy**：LLDP-MED ネットワーク ポリシー TLV • **power-management**：LLDP-MED 電源管理 TLV
receive	LLDP 伝送を受信するようにインターフェイスをイネーブルにします。
tlv-select	送信する LLDP TLV を選択します。
power-management	LLDP 電源管理 TLV を送信します。
transmit	インターフェイスで LLDP 伝送をイネーブルにします。

コマンド デフォルト

サポート対象のインターフェイスで LLDP 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
Cisco IOS XE 3.2SE	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、802.1 メディア タイプでサポートされています。

インターフェイスがトンネル ポートに設定されていると、LLDP は自動的にディセーブルになります。

インターフェイスの LLDP 伝送をディセーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no lldp transmit
```

インターフェイスの LLDP 伝送をイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# lldp transmit
```

logging event power-inline-status

Power over Ethernet（PoE）イベントのロギングを有効にするには、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 power-inline-status** 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無効にするには、このコマンドの **no** 形式を使用します。

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。

コマンド 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
Cisco IOS XE 3.2SE	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 **no** 形式を使用しても、PoE エラー イベントは無効になりません。

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。

```
Device(config-if)# interface gigabitethernet1/0/1
Device(config-if)# logging event power-inline-status
Device(config-if)#
```

関連トピック

power inline, （173 ページ）
show power inline, （242 ページ）

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。Auto MDIX をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdix auto

no mdix auto

構文の説明

このコマンドには引数またはキーワードはありません。

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
Cisco IOS XE 3.2SE	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。

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。

インターフェイスの Auto-MDIX の動作ステートを確認するには、**show controllers ethernet-controller** *interface-id* **phy** 特権 EXEC コマンドを入力します。

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。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto
Device(config-if)# duplex auto
Device(config-if)# mdix auto
Device(config-if)# end
```

関連トピック

show controllers ethernet-controller, （183 ページ）

mode（電源スタックの設定）

設定内容 電源スタックの電源スタックモードを設定するには、電源スタック コンフィギュレーション モードで **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。

mode {**power-shared**| **redundant**} **[strict]**

no mode

構文の説明

power-shared	電源スタックが電源共有モードで動作するよう、設定します。これはデフォルトです。
redundant	電源スタックが冗長モードで動作するよう、設定します。他の電源の 1 つに障害が発生した場合のバックアップ電源として使用するため、最大の電源が電源プールから削除されます。
strict	（任意）電力バジェットが正確に実行されるよう、電源スタック モードを設定します。スタック電力は、使用可能電力を超えることができません。

コマンド デフォルト

デフォルト モードは **power-shared** および nonstrict です。

コマンド モード

電源スタックの設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、IP Base または IP Services フィーチャ セットが実行されているスイッチ スタックでのみ使用できます。

電源スタック コンフィギュレーション モードにアクセスするには、**stack-power stack** *power stack 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。

no mode コマンドを入力すると、スイッチが、デフォルトの **power-shared** モードおよび non-strict モードに設定されます。

（注） スタック電源の場合、使用可能電力は、PoE で使用できる、電源スタックのすべての電源からの合計電力です。使用可能電力は、スタックの PoE ポートに接続されているすべての受電デバイスに割り当てられている電力です。消費電力は、受電デバイスで実際に消費される電力です。

power-shared モードでは、すべての入力電力を負荷に使用でき、使用可能な合計電力は 1 つの大きな電源として扱われます。電力バジェットには、すべての電源から供給されるすべての電力が含まれます。電源障害の場合に除外される電力はありません。電源に障害が発生した場合、負荷制限（受電デバイスまたはスイッチのシャットダウン）が発生する場合があります。

redundant モードでは、他の電源の 1 つに障害が発生した場合のバックアップ電源として使用するため、最大の電源が電源プールから削除されます。使用可能な電力バジェットは、合計電力から最大の電源を差し引いたものです。これによって、スイッチおよび受電デバイスのプールで使用できる電力が減少しますが、障害または過剰な電力負荷が発生した場合に、スイッチまたは受電デバイスのシャットダウンの必要性が小さくなります。

strict モードでは、電源に障害が発生し、使用可能な電力が電力バジェットを下回った場合、システムによって、実際の電力が使用可能な電力よりも少ないかのように、受電デバイスの負荷制限を介してバジェットのバランスがとられます。nonstrict モードでは、電源スタックは割り当て超過状態で実行でき、実際の電力が使用可能な電力を超過しない限り、安定しています。このモードでは、受電デバイスが通常の電力を超えて電力を引き出すと、電源スタックが負荷制限を開始することがあります。ほとんどの装置は全出力電力では実行されないため、これは、通常、問題ではありません。スタック内で同時に最大電力を必要とする複数の受電デバイスが存在する可能性は、小さいからです。

strict モードと nonstrict モードの両方とも、電力バジェットに使用可能な電力がなくなった時点で、電力は拒否されます。

次に、power1 という名前のスタックの電源スタックモードを、電力バジェットを strict にした power-shared に設定する例を示します。スタック内のすべての電力は共有されますが、使用可能な電力全体が割り当てられた場合、電力を使用できる余分な装置はなくなります。

```
Device(config)# stack-power stack power1
Device(config-stackpower)# mode power-shared strict
Device(config-stackpower)# exit
```

次に、power2 という名前のスタックの電源スタックモードを redundant に設定する例を示します。スタック内の最大の電源は電源プールから削除され、他の電源の 1 つが発生した場合に冗長性が提供されます。

```
Device(config)# stack-power stack power2
Device(config-stackpower)# mode redundant
Device(config-stackpower)# exit
```

関連トピック

stack-power , （256 ページ）

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には、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	インターフェイスに適用する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
Cisco IOS XE 3.2SE	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。

最初にネットワークポリシー プロファイルを設定する場合、インターフェイスに **switchport voice vlan** コマンドを適用できません。ただし、**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、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。

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。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# network-policy 60
```

関連トピック

network-policy profile（グローバル コンフィギュレーション）, （168 ページ）

show network-policy profile, （223 ページ）

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。ポリシーを削除して、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。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
Cisco IOS XE 3.2SE	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 モードを開始するには、**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。

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。

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。

```
Device(config)# network-policy profile 60
Device(config-network-policy)#
```

関連トピック

network-policy, （167 ページ）

show network-policy profile, （223 ページ）

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。デフォルト設定に戻すには、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

インターフェイス 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
Cisco IOS XE 3.2SE	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 モビリティ サービス エンジン（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。

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。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# nmsp attachment suppress
```

関連トピック

show nmsp

power efficient-ethernet auto

インターフェイスの EEE 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 **power efficient-ethernet auto** コマンドを使用します。インターフェイスで EEE をディセーブルにするには、このコマンドの **no** 形式を使用します。

power efficient-ethernet auto

no power efficient-ethernet 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

EEE 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い使用率のときに LPI モードを開始して、電力を節約できます。LPI モードでは、リンクの両端にあるシステムは、特定のサービスをシャットダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

インターフェイスが EEE に対応している場合にのみ、**power efficient-ethernet auto** コマンドを使用できます。インターフェイスが EEE に対応しているかどうかを確認するには、**show eee capabilities** EXEC コマンドを使用します。

EEE がイネーブルの場合、デバイスはリンク パートナーに EEE をアドバタイズし、自動ネゴシエートします。インターフェイスの現在の EEE ステータスを表示するには、**show eee status** EXEC コマンドを使用します。

このコマンドにライセンスは必要ありません。

次に、インターフェイスで EEE をイネーブルにする例を示します。

```
Device(config-if)# power efficient-ethernet auto
Device(config-if)#
```

次に、インターフェイスで EEE をディセーブルにする例を示します。

```
Device(config-if)# no power efficient-ethernet auto
Device(config-if)#
```

power-priority

電源スタックのスイッチと高プライオリティおよび低プライオリティ PoE ポートに対して、Cisco StackPower の電源プライオリティ値を設定するには、スイッチ スタック電源コンフィギュレーション モードで **power-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。

power-priority {**high** *value*| **low** *value*| **switch** *value*}

no power-priority {**high**| **low**| **switch**}

構文の説明

high *value*	ポートの電力プライオリティを高プライオリティポートとして設定します。値は 1 ～ 27 です。1 が最高のプライオリティです。**high** の値は、低プライオリティポートに設定する値よりも小さく、スイッチに設定する値よりも大きくする必要があります。
low *value*	ポートの電力プライオリティを低プライオリティポートとして設定します。指定できる範囲は 1 ～ 27 です。**low** の値は、高プライオリティ ポートおよびスイッチに設定された値よりも大きくする必要があります。
switch *value*	スイッチの電力プライオリティを設定します。指定できる範囲は 1 ～ 27 です。**switch** の値は、低プライオリティポートおよび高プライオリティポートに設定された値よりも小さくする必要があります。

コマンド デフォルト

値が設定されていない場合、電源スタックでは、デフォルト プライオリティがランダムに決定されます。

デフォルトの範囲は、スイッチで 1 ～ 9、高プライオリティ ポートで 10 ～ 18、低プライオリティポートで 19 ～ 27 です。

非 PoE スイッチでは、（ポート プライオリティの）高い値と低い値は、影響がありません。

コマンド モード

スイッチのスタック電源設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 スタック電源コンフィギュレーション モードにアクセスするには、**stack-power switch***switch-number* 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。

Cisco StackPower の電源プライオリティ値によって、電源が失われ、負荷制限が発生した場合のスイッチとポートのシャットダウンの順序が決定されます。プライオリティ値は 1 ～ 27 です。最も高い数が最初にシャットダウンされます。

各スイッチ、その高プライオリティポート、および低プライオリティポートでは、異なるプライオリティ値を設定して、電源が失われている間に一度にシャットダウンされる装置数を制限することを推奨します。同じ電源スタックの異なるスイッチに同じプライオリティ値を設定しようとすると、設定は許可されますが、警告メッセージが表示されます。

（注） このコマンドは、IP Base または IP Services フィーチャ セットが実行されているスイッチ スタックでのみ使用できます。

次に、電源スタックの switch 1 の電源プライオリティを 7 に、高プライオリティ ポートを 11 に、低プライオリティ ポートを 20 に設定する例を示します。

```
Device(config)# stack-power switch 1
Device(config-switch-stackpower)# stack-id power_stack_a
Device(config-switch-stackpower)# power-priority high 11
Device(config-switch-stackpower)# power-priority low 20
Device(config-switch-stackpower)# power-priority switch 7
Device(config-switch-stackpower)# exit
```

関連トピック

show stack-power

stack-power , （256 ページ）

power inline

Power over Ethernet（PoE）ポートで電源管理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 **power inline** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

power inline {**auto** [**max** *max-wattage*]| **four-pair forced**| **never**| **port priority** {**high**| **low**} | **static** [**max** *max-wattage*]}

no power inline {**auto**| **four-pair forced**| **never**| **port priority** {**high**| **low**}| **static** [**max** *max-wattage*]}

構文の説明

auto	受電装置の検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。割り当ては、検出された順序で行われます。
max*max-wattage*	（任意）ポートに供給される電力を制限します。指定できる範囲は 4000 ～ 30000 mW です。値を指定しない場合は、最大電力が供給されます。

four-pair forced	（任意）L2 ネゴシエーションなしで 4 ペア PoE をイネーブルにします（Cisco UPOE スイッチのみ）。
never	装置の検出とポートへの電力供給をディセーブルにします。
port	ポートの電源プライオリティを設定します。デフォルトの優先度は [Low] です。
priority{**high**|**low**}	ポートの電源プライオリティを設定します。電源に障害が発生した場合には、低プライオリティとして設定されているポートが最初にオフになり、高プライオリティとして設定されたポートは最後にオフになります。デフォルトの優先度は [Low] です。
static	受電装置の検出をイネーブルにします。スイッチが受電デバイスを検出する前に、ポートへの電力を事前に割り当てます（確保します）。このアクションによって、インターフェイスに接続されたデバイスで十分な電力を受け取ることができます。

コマンド 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、30,000 mW です。

デフォルトのポート プライオリティは低です。

コマンド デフォルト

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**four-pair forced** キーワードが追加されました。

使用上のガイドライン

このコマンドは、PoE対応ポートだけでサポートされています。PoEがサポートされていないポートでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline auto
                   ^
% Invalid input detected at '^' marker.
```

スイッチ スタックでは、このコマンドはPoEをサポートしているスタックの全ポートでサポートされます。

Cisco Universal Power Over Ethernet（Cisco UPOE）は、シグナル ペア（導線 1、2、3、6）付きのRJ-45 ケーブルのスペア ペア（導線 4、5、7、8）を使用して、IEEE 802.at PoE 標準を拡張するシスコ独自のテクノロジーで、標準のイーサネット ケーブル配線インフラストラクチャ（クラス D 以上）により最大60 Wの電力を供給する機能を提供します。スペア ペアの電力は、スイッチ ポートとエンドデバイスがCisco UPOE対応であることをCDPまたはLLDPを使用して相互に識別し、エンドデバイスがスペア ペアの電力のイネーブル化を要求したときにイネーブルになります。スペア ペアに給電されると、エンドデバイスは、CDP または LLDP を使用して、スイッチから最大 60 W の電力をネゴシエートできます。**power inline four-pair forced** コマンドは、信号ペアおよびスペア ペアの両方のエンド デバイスが PoE 対応の場合に使用します。ただし、Cisco UPOE に必要な CDP または LLDP 拡張はサポートしていません。

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 30 W 未満に設定されている場合、スイッチは Class 0 または Class 3 装置に電力を供給しません。

スイッチが受電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** 特権 EXEC コマンド出力の Oper カラムに *power-deny* が表示されます。

ポートに高いプライオリティを与えるには、**power inline static max***max-wattage* コマンドを使用します。スイッチは、auto モードに設定されたポートに電力を割り当てる前に、static モードに設定されたポートに PoE を割り当てます。スイッチは、装置検出より優先的に設定されている場合に、スタティック ポートの電力を確保します。接続された装置がない場合は、ポートがシャットダウン状態か否かに関係なく、スタティック ポートの電力が確保されます。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電デバイスからの 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されているので、最大ワット数以下の電力を使用する受電デバイスは、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、ポートは設定された速度とデュプレックス設定を使用して自動ネゴシエーションします。これは、受電デバイスであるかどうかに関係なく、接続された装置の電力要件を判別するのに必要です。電力要件が判別された後、スイッチはインターフェイスをリセットすることなく、設定された速度とデュプレックス設定を使用してインターフェイスをハードコードします。

power inline never コマンドを使用してポートを設定すると、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。不正なリンクアップが生じ、ポートが errdisable ステートになる可能性があります。

power inline port priority {high | low} コマンドを使用して、PoE ポートの電源プライオリティを設定します。電力が不足した場合には、低いポート プライオリティでポートに接続されている受電デバイスが、まず、シャットダウンされます。

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

次の例では、スイッチ上で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。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto
```

次に、スイッチ ポート ギガビット イーサネット 1/0/1 から自動的に信号ペアおよびスペア ペアの両方の電力をイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline four-pair forced
```

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、スイッチ上で PoE ポートを設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、スイッチ上で PoE ポートへの電力供給を停止する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline never
```

次の例では、電源に障害が発生した場合に最後のポートの1つがシャットダウンされるよう、ポートのプライオリティを高に設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline port priority high
```

関連トピック

logging event power-inline-status, （163 ページ）

show power inline, （242 ページ）

power inline police

受電デバイスでリアルタイム電力消費のポリシングをイネーブルにするには、インターフェイスコンフィギュレーションモードで **power inline police** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

power inline police [**action** {**errdisable**| **log**}]

no power inline police

構文の説明

action errdisable	（任意）リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、ポートへの電力をオフにするよう、デバイスを設定します。これがデフォルトのアクションになります。
action log	（任意）リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、接続されているデバイスへの電力を供給しながら、デバイスが Syslog メッセージを生成するように設定します。

コマンド デフォルト

受電デバイスのリアルタイムの電力消費のポリシングは、ディセーブルです。

コマンド モード

インターフェイス 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
Cisco IOS XE 3.2SE	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、LAN Base イメージのみでサポートされています。

このコマンドは、Power of Ethernet（PoE）対応ポートのみでサポートされています。PoE をサポートしていないデバイスまたはポートでこのコマンドを入力すると、エラー メッセージが表示されます。

スイッチ スタックでは、このコマンドは、PoEおよびリアルタイム電力消費モニタリングをサポートしているスタックの全スイッチまたはポートでサポートされます。

リアルタイムの電力消費のポリシングがイネーブルである場合、受電デバイスが割り当てられた最大電力より多くの量を消費すると、デバイスが対処します。

PoE がイネーブルである場合、デバイスは受電装置のリアルタイムの電力消費を検知します。この機能は、パワーモニタリングまたはパワーセンシングといわれます。また、デバイスはパワーポリシング機能を使用して消費電力をポリシングします。

パワー ポリシングがイネーブルである場合、デバイスは次の順のいずれかの方式で PoE ポートのカットオフ電力として、これらの値の 1 つを使用します。

1. **power inline auto max***max-wattage* または **power inline static max***max-wattage* インターフェイス コンフィギュレーション コマンドを入力する場合、ポートで許可する電力を制限するユーザ定義の電力レベル。
2. デバイスでは、CDP パワー ネゴシエーションまたは IEEE 分類および LLPD 電力ネゴシエーションを使用して、装置の消費使用量が自動的に設定されます。

カットオフ電力量の値を手動で設定しない場合、デバイスは、CDP 電力ネゴシエーションまたはデバイスの IEEE 分類と LLDP 電力ネゴシエーションを使用して自動的に値を決定します。CDP または LLDP がイネーブルでない場合は、デフォルト値の 30 W が適用されます。ただし、CDP または LLDP がない場合は、15400 ～ 30000 mW の値が CDP 要求または LLDP 要求だけに基づいて割り当てられるため、装置で 15.4 W を超える電力の消費がデバイスから許可されません。受電デバイスが CDP または LLDP のネゴシエーションなしに 15.4 W を超える電力を消費する場合、装置は最大電流 *Imax* の制限に違反し、最大値を超える電流が供給されるという *Icut* 障害が発生する可能性があります。再び電源を入れるまで、ポートは障害状態のままになります。ポートで継続的に 15.4 W を超える電力が給電される場合、このサイクルが繰り返されます。

PoE+ ポートに接続されている受電デバイスが再起動し、電力 TLV で CDP パケットまたは LLDP パケットが送信される場合、デバイスは最初のパケットの電力ネゴシエーション プロトコルをロックし、その他のプロトコルからの電力要求に応答しません。たとえば、デバイスが CDP にロックされている場合、LLDP要求を送信する装置に電力を供給しません。デバイスがCDPにロッ

クされた後でCDPがディセーブルになった場合、デバイスはLLDP電源要求に応答せず、アクセサリの電源がオンにならなくなります。この場合、受電デバイスを再起動する必要があります。

パワーポリシングがイネーブルである場合、デバイスはリアルタイムの電力消費をPoEポートに割り当てられた最大電力と比較して、消費電力をポリシングします。装置が最大電力割り当て（またはカットオフ電力）を超える電力をポートで使用している場合、デバイスでは、ポートへの電力供給がオフにされるか、または装置に電力を供給しながらデバイスはSyslogメッセージが生成してLED（ポートLEDはオレンジ色に点滅）を更新します。

- ポートへの電力供給をオフにして、ポートをerror-disabledステートとするようデバイスを設定するには、**power inline police** インターフェイス コンフィギュレーション コマンドを使用します。
- 装置に電力を供給しながら、syslogメッセージを生成するようデバイスを設定するには、**power inline police action log** コマンドを使用します。

action log キーワードを入力しない場合のデフォルトのアクションは、ポートのシャットダウン、ポートへの電力供給のオフ、およびポートをPoE error-disabledステートに移行になります。PoEポートをerror-disabledステートから自動的に回復するよう設定するには、**errdisable detect cause inline-power** グローバル コンフィギュレーション コマンドを使用して、PoE原因に対するerror-disabled検出をイネーブルにして、**errdisable recovery cause inline-power interval***interval* グローバル コンフィギュレーション コマンドを使用して、PoE error-disabled原因の回復タイマーをイネーブルにします。

注意 ポリシングがディセーブルである場合、受電デバイスがポートに割り当てられた最大電力より多くの量を消費しても対処されないため、デバイスに悪影響を与える場合があります。

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

次の例では、電力消費のポリシングをイネーブルにして、デバイスのPoEポートでSyslogメッセージを生成するようデバイスを設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline police action log
```

関連トピック

power inline, （173 ページ）
show power inline, （242 ページ）

電源装置

スイッチの内部電源を設定および管理するには、特権EXECモードで **power supply** コマンドを使用します。

power supply *stack-member-number* **slot** {**A**| **B**} {**off**| **on**}

構文の説明

stack-member-number	内部電源を設定するスタック メンバ番号。指定できる範囲は、スタック内のスイッチの数に応じて 1 ～ 9 です。 このパラメータは、スタック対応スイッチだけで使用できます。
slot	設定するスイッチの電源を選択します。
A	スロット A の電源を選択します。
B	スロット B の電源を選択します。 （注） 電源スロット B は、スイッチの外側エッジに最も近いスロットです。
off	スイッチの電源をオフに設定します。
on	スイッチの電源をオンに設定します。

コマンド デフォルト

スイッチの電源がオンになります。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**slot** キーワードが **frufep** キーワードに代わるものとして使用されるようになりました。

使用上のガイドライン

power supply コマンドは、スイッチまたはすべてのスイッチが同じプラットフォームであるスイッチ スタックに適用されます。

同じプラットフォーム スイッチを含むスイッチ スタックでは、**slot** {**A** | **B**}**off** or **on** キーワードを入力する前に、スタック メンバを指定する必要があります。

デフォルト設定に戻すには、**power supply***stack-member-number***on** コマンドを使用します。

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

次に、スロット A の電源装置をオフに設定する例を示します。

```
Device> power supply 2 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Device
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
```

次に、スロット A の電源装置をオンに設定する例を示します。

```
Device> power supply 1 slot B on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

次に、show env power コマンドの出力例を示します。

```
Device> show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  PWR-1RUC2-640WAC    DCB1705B05B OK               Good     Good     250/390
1B  Not Present
```

show CAPWAP summary

アクセスポイントおよびその他のモビリティ コントローラに対してコントローラが確立するすべての CAPWAP トンネルを表示するには、**show CAPWAP summary** コマンドを使用します。

show CAPWAP summary

構文の説明

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

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントなどに対して、コントローラの確立する CAPWAP トンネルを表示する例を示します。

```
Device# show capwap summary
CAPWAP Tunnels General Statistics:
Number of Capwap Data Tunnels = 8
Number of Capwap Mobility Tunnels = 0
Number of Capwap Multicast Tunnels = 0
Name APName Type PhyPortIf Mode McastIf
------ -------------------------------- ---- --------- ---------
-------
Ca4 AP-Behind-Router data - unicast -
Ca0 AP1142-kat data - unicast -
Ca5 APRFCHAMBER2-EDISON data - unicast -
Ca6 KATANA_2_RF data - unicast -
Ca1 AP-1040-RF data - unicast -
Ca7 KATANA_1_RF data - unicast -
Ca2 AP3500-2027 data - unicast -
Ca3 AP-1040-out data - unicast -
```

show controllers cpu-interface

CPU ネットワーク インターフェイス 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 [**switch** *stack-member-number*]

構文の説明

switch *stack-member-number*	（任意）スタック メンバ番号を指定します。

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
Cisco IOS XE 3.2SE	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。

次に、**show controllers cpu-interface** コマンドの一部の出力例を示します。

```
Device# show controllers cpu-interface switch 1
cpu-queue-frames  retrieved dropped invalid hol-block

----------------  --------- ------- ------- ---------

Routing Protocol          0         0     0     0
L2 Protocol          241567         0     0     0
sw forwarding             0         0     0     0
broadcast             68355         0     0     0
icmp                      0         0     0     0
icmp redirect             0         0     0     0
logging                   0         0     0     0
rpf-fail                  0         0     0     0
DOT1X authentication 328174         0     0     0
Forus Traffic             0         0     0     0
Forus Resolution          0         0     0     0
Wireless q5               0         0     0     0
Wireless q1               0         0     0     0
Wireless q2               0         0     0     0
Wireless q3               0         0     0     0
Wireless q4               0         0     0     0
Learning cache            0         0     0     0
Topology control     820408         0     0     0
Proto snooping            0         0     0     0
BFD Low latency           0         0     0     0
Transit Traffic           0         0     0     0
Multi End station         0         0     0     0
Health Check              0         0     0     0
Crypto control            0         0     0     0
Exception                 0         0     0     0
General Punt              0         0     0     0
NFL sampled data          0         0     0     0
STG cache                 0         0     0     0
EGR exception             0         0     0     0
show forward              0         0     0     0
Multicast data            0         0     0     0
Gold packet               0         0     0     0
```

関連トピック

show controllers ethernet-controller, （183 ページ）

show interfaces, （205 ページ）

show controllers ethernet-controller

キーワードでハードウェアから読み込んだインターフェイス単位の送受信の統計情報を表示するには、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*] [**down-when-looped**| **phy** [**detail**]] [**port-asic statistics** {**exceptions**| **interface** *interface-id* {**l2**| **l3**}| **l3-ifid** *if-id*| **port-ifid** *if-id*| **vlan-ifid** *if-id*} [**switch** *stack-member-number*] [**asic** *asic-number*]]

構文の説明

interface-id	（任意）物理インターフェイスの ID です。
down-when-looped	（任意）down-when-looped 検出に関連するステートを表示します。

phy	（任意）デバイス、またはインターフェイスのスイッチの物理層デバイス（PHY）の内部レジスタ ステータスを表示します。インターフェイスの Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能の動作ステートを表示に含めます。
detail	（任意）PHY 内部レジスタの詳細情報を表示します。
port-asic	（任意）ポートの ASIC 内部レジスタの情報を表示します。
statistics	ポートの ASIC 統計情報（Rx/Sup キューおよびその他の統計情報を含む）を表示します。
exceptions	ポートの ASIC 例外統計情報を表示します。
interface *interface-id*	ポートの ASIC 統計情報を表示するインターフェイスを指定します。
l2	レイヤ 2 インターフェイスの統計情報を表示します。
l3	レイヤ 3 インターフェイスの統計情報を表示します。
l3-ifid *if-id*	ポートの ASIC 統計情報を表示するレイヤ 3 IF インターフェイス ID を指定します。
port-ifid *if-id*	ポートの ASIC 統計情報を表示する PortIF インターフェイス ID を指定します。
vlan-ifid *if-id*	ポートの ASIC 統計情報を表示する VLANIF インターフェイス ID を指定します。
switch *stack-member-number*	（任意）送受信の統計情報を表示するスタック メンバ番号を指定します。
asic *asic-number*	（任意）ASIC 番号を指定します。

コマンド モード

ユーザ EXEC（ユーザ EXEC モードの *interface-id* キーワードを指定した場合だけサポート）

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

キーワードがない場合、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 RMON 統計情報を示します。

インターフェイスの内部レジスタを表示するには、**phy** キーワードを使用します。ポートの ASIC に関する情報を表示するには、**port-asic** キーワードを使用します。

phy または **port-asic** キーワードを入力すると、主にシスコ テクニカル サポート担当者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。

次に、あるインターフェイスに対する **show controllers ethernet-controller** コマンドの出力例を示します。

```
Device# show controllers ethernet-controller gigabitethernet1/0/1
Transmit                  GigabitEthernet1/0/1          Receive
   19216827 Total bytes                                0 Total bytes
      41935 Unicast frames                             0 Unicast frames
    2683840 Unicast bytes                              0 Unicast bytes
     216662 Multicast frames                           0 Multicast frames
   16532987 Multicast bytes                            0 Multicast bytes
          0 Broadcast frames                           0 Broadcast frames
          0 Broadcast bytes                            0 Broadcast bytes
          0 System FCS error frames                    0 IpgViolation frames
          0 MacUnderrun frames                         0 MacOverrun frames
          0 Pause frames                               0 Pause frames
          0 Cos 0 Pause frames                         0 Cos 0 Pause frames
          0 Cos 1 Pause frames                         0 Cos 1 Pause frames
          0 Cos 2 Pause frames                         0 Cos 2 Pause frames
          0 Cos 3 Pause frames                         0 Cos 3 Pause frames
          0 Cos 4 Pause frames                         0 Cos 4 Pause frames
          0 Cos 5 Pause frames                         0 Cos 5 Pause frames
          0 Cos 6 Pause frames                         0 Cos 6 Pause frames
          0 Cos 7 Pause frames                         0 Cos 7 Pause frames
          0 Oam frames                                 0 OamProcessed frames
          0 Oam frames                                 0 OamDropped frames
     251598 Minimum size frames                        0 Minimum size frames
          0 65 to 127 byte frames                      0 65 to 127 byte frames
          0 128 to 255 byte frames                     0 128 to 255 byte frames
       6999 256 to 511 byte frames                     0 256 to 511 byte frames
          0 512 to 1023 byte frames                    0 512 to 1023 byte frames
          0 1024 to 1518 byte frames                   0 1024 to 1518 byte frames
          0 1519 to 2047 byte frames                   0 1519 to 2047 byte frames
          0 2048 to 4095 byte frames                   0 2048 to 4095 byte frames
          0 4096 to 8191 byte frames                   0 4096 to 8191 byte frames
          0 8192 to 16383 byte frames                  0 8192 to 16383 byte frames
          0 16384 to 32767 byte frame                  0 16384 to 32767 byte frame
          0 > 32768 byte frames                        0 > 32768 byte frames
          0 Late collision frames                      0 SymbolErr frames
          0 Excess Defer frames                        0 Collision fragments
          0 Good (1 coll) frames                       0 ValidUnderSize frames
          0 Good (>1 coll) frames                      0 InvalidOverSize frames
          0 Deferred frames                            0 ValidOverSize frames
          0 Gold frames dropped                        0 FcsErr frames
          0 Gold frames truncated
          0 Gold frames successful
          0 1 collision frames
          0 2 collision frames
          0 3 collision frames
          0 4 collision frames
          0 5 collision frames
          0 6 collision frames
          0 7 collision frames
          0 8 collision frames
          0 9 collision frames
          0 10 collision frames
          0 11 collision frames
```

```
          0 12 collision frames
          0 13 collision frames
          0 14 collision frames
          0 15 collision frames
          0 Excess collision frames

LAST UPDATE 850 msecs AGO
```

表 *11*：*Transmit* のフィールドの説明

フィールド	説明
Total 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。
Unicast bytes	ユニキャスト アドレスに送信されたバイトの総数。
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。
Multicast bytes	マルチキャスト アドレスに送信されたバイトの総数。
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。
Broadcast bytes	ブロードキャスト アドレスに送信されたバイトの総数。
System FCS error frames	フレーム チェック シーケンス（FCS）に失敗したフレームの総数。
MacUnderrun frames	MAC アンダーラン エラーを持つフレームの総数。
Pause frames	インターフェイス上で送信されたポーズ フレームの総数。
Cos x Pause frames	インターフェイス上で送信されたサービス クラス（CoS）X ポーズ フレームの総数。
Oam frames	インターフェイス上で送信されたイーサネット OAM（オペレーション、アドミニストレーション、およびメンテナンス）フレームの総数。
Minimum size frames	最小許可フレーム サイズのフレームの数。
65 to 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。
128 to 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。
256 to 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。

フィールド	説明
512 to 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。
1024 to 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。
1519 to 2047 byte frames	インターフェイス上で送信された 1519 ～ 2047 バイトのフレームの総数。
2048 to 4095 byte frames	インターフェイス上で送信された 2048 ～ 4095 バイトのフレームの総数。
4096 to 8191 byte frames	インターフェイス上で送信された 4096 ～ 8191 バイトのフレームの総数。
8192 to 16383 byte frames	インターフェイス上で送信された 8192 ～ 16383 バイトのフレームの総数。
16384 to 32767 byte frames	インターフェイス上で送信された 16384 ～ 32767 バイトのフレームの総数。
> 32768 byte frames	インターフェイス上で送信された 32768 バイトより大きいフレームの総数。
Late collision frames	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。
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。
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。
Good (>1 coll) frames	2 回以上の衝突後、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 2 回以上の衝突後、正常に送信されなかったフレームの数は含まれません。
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。
Gold frames dropped	ドロップされたゴールド フレームの数。
Gold frames truncated	切り捨てられたゴールド フレームの数。

フィールド	説明
Gold frames successful	成功したゴールド 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。
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。

フィールド	説明
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。
Excess 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。

表 *12* : *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。

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 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。[1]。

フィールド	説明
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

表 *13* : *Receive* のフィールドの説明

フィールド	説明
Total 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 値および正常形式でないフレームも含まれます。[2]。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。

フィールド	説明
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。
Multicast frames	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。
Multicast bytes	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バイトの総数。
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。
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。
IpgViolation frames	パケット間ギャップ（IPG）違反のフレームの総数。
MacOverrun frames	MacOverrun エラーのフレームの総数。
Pause frames	インターフェイス上で受信されたポーズ フレームの総数。
Cos x Pause frames	インターフェイス上で受信されたサービス クラス（CoS）X ポーズ フレームの総数。
OamProcessed	インターフェイス上で処理されたイーサネット OAM（オペレーション、アドミニストレーション、およびメンテナンス）フレームの総数。
OamDropped	インターフェイス上でドロップされたイーサネット OAM（オペレーション、アドミニストレーション、およびメンテナンス）フレームの総数。
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。

フィールド	説明
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。
1519 to 2047 byte frames	1519 ～ 2047 バイトのフレームの総数。
2048 to 4095 byte frames	2048 ～ 4095 バイトのフレームの総数。
4096 to 8191 byte frames	4096 ～ 8191 バイトのフレームの総数。
8192 to 16383 byte frames	8192 ～ 16383 バイトのフレームの総数。
16384 to 32767 byte frames	16384 ～ 32767 バイトのフレームの総数。
> 32768 byte frames	32768 バイトより大きいフレームの総数。
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。
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。
Valid undersize frames	64 バイト（または VLAN タグ付きフレームでは 68 バイト）未満で、有効なFCS値を持つインターフェイスで受信されたフレームの数。フレーム サイズには、FCS ビットが含まれ、フレーム ヘッダー ビットは含まれません。
Invalid oversize frames	許可される最大伝送単位（MTU）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 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。
FcsErr 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。

[2] FCS = フレーム チェック シーケンス

次に、特定のインターフェイスに対する **show controllers ethernet-controller phy** コマンドの出力例を示します。

```
Device# show controllers ethernet-controller gigabitethernet1/0/2 phy
Gi1/0/2 (gpn: 2, port-number: 2)
------------------------------------------------------------
 0000 : 1140  Control Register                   :  0001 0001 0100 0000
 0001 : 7949  Control STATUS                     :  0111 1001 0100 1001
 0002 : 0141  Phy ID 1                           :  0000 0001 0100 0001
 0003 : 0EE0  Phy ID 2                           :  0000 1110 1110 0000
 0004 : 03E1  Auto-Negotiation Advertisement     :  0000 0011 1110 0001
 0005 : 0000  Auto-Negotiation Link Partner      :  0000 0000 0000 0000
 0006 : 0004  Auto-Negotiation Expansion Reg     :  0000 0000 0000 0100
 0007 : 2001  Next Page Transmit Register        :  0010 0000 0000 0001
 0008 : 0000  Link Partner Next page Registe     :  0000 0000 0000 0000
 0010 : 3B60  PHY Specific Control               :  0011 1011 0110 0000
 0011 : 8010  PHY Specific Status                :  1000 0000 0001 0000
 0012 : 6404  PHY Specific Interrupt Enable      :  0110 0100 0000 0100
 0013 : 0000  PHY Specific Interrupt Status      :  0000 0000 0000 0000
```

関連トピック

show controllers cpu-interface, （182 ページ）

show controllers cpu-interface, （182 ページ）

show controllers utilization

帯域幅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）物理インターフェイスの ID です。

コマンド デフォルト

なし

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show controllers utilization** コマンドの出力例を示します。

```
Device> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Gi1/0/1             0                    0
Gi1/0/2             0                    0
Gi1/0/3             0                    0
Gi1/0/4             0                    0
Gi1/0/5             0                    0
Gi1/0/6             0                    0
Gi1/0/7             0                    0
<output truncated>
Gi2/0/1             0                    0
Gi2/0/2             0                    0
<output truncated>
Total Ports : 48
Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Average Switch Percentage Utilization : 0
```

次に、特定のポートでの **show controllers utilization** コマンドの出力例を示します。

```
Device> show controllers gigabitethernet1/0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

表 *14*：*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。
Average Switch 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。

show eee

インターフェイスの EEE 情報を表示するには、EXEC モードで **show eee** コマンドを使用します。

show eee{**capabilities**| **status**}**interface***interface-id*

構文の説明

capabilities	指定インターフェイスの EEE 機能を表示します。

status	指定したインターフェイスのEEEステータス情報を表示します。
interface *interface-id*	EEE機能またはステータス情報を表示するための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

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い電力使用率のときにLPIモードを開始して、電力を節約できます。LPIモードでは、リンクの両端にあるシステムは、特定のサービスをシャットダウンして、電力を節約できます。EEEは上位層プロトコルおよびアプリケーションに対して透過的であるように、LPIモードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

インターフェイスが EEE に対応しているかどうかを確認するには、**show eee capabilities** コマンドを使用します。**power efficient-ethernet auto** インターフェイス コンフィギュレーション コマンドを使用して、EEE に対応しているインターフェイスで EEE をイネーブルにできます。

インターフェイスの EEE ステータス、LPI ステータス、および wake エラー カウント情報を表示するには、**show eee status** コマンドを使用します。

次の例では、EEE がイネーブルのインターフェイスの **show eee capabilities** コマンドの出力を示します。

```
Device# show eee capabilities interface gigabitethernet1/0/1
Gi1/0/1
        EEE(efficient-ethernet):  yes (100-Tx and 1000T auto)
        Link Partner            :  yes (100-Tx and 1000T auto)
```

次の例では、EEE がイネーブルでないインターフェイスの **show eee capabilities** コマンドの出力を示します。

```
Device# show eee capabilities interface gigabitethernet2/0/1
Gi2/0/1
        EEE(efficient-ethernet):  not enabled
        Link Partner            :  not enabled
```

次の例では、EEE がイネーブルで機能しているインターフェイスの **show eee status** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device# show eee status interface gigabitethernet1/0/4
Gi1/0/4 is up
        EEE(efficient-ethernet):  Operational
        Rx LPI Status           :  Received
        Tx LPI Status           :  Received
```

次の例では、EEE が機能していて、ポートが節電モードであるインターフェイスの **show eee status** コマンドの出力を示します。

```
Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is up
        EEE(efficient-ethernet):  Operational
        Rx LPI Status           :  Low Power
        Tx LPI Status           :  Low Power
        Wake Error Count        :  0
```

次の例では、リモート リンク パートナーが EEE と互換性がないために、EEE がイネーブルでないインターフェイスの **show eee status** コマンドの出力を示します。

```
Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is down
        EEE(efficient-ethernet):  Disagreed
        Rx LPI Status           :  None
        Tx LPI Status           :  None
        Wake Error Count        :  0
```

表 *15* : ***show eee status*** のフィールドの説明

フィールド	説明
EEE (efficient-ethernet)	インターフェイスのEEEステータス。このフィールドには、次のいずれかの値を使用できます。 • N/A：ポートは EEE に対応できません。 • Disabled：ポートの EEE はディセーブルです。 • Disagreed：リモート リンク パートナーが EEE に互換性がない可能性があるため、ポートの EEE は設定されていません。EEE 対応でないか、EEE の設定に互換性がありません。 • Operational：ポートの EEE がイネーブルで機能しています。 インターフェイスの速度が 10 Mbps として設定されていると、EEE は内部的にディセーブルになります。インターフェイスの速度が auto、100 Mbps または 1000 Mbps に戻ると、EEE は再びアクティブになります。

フィールド	説明
Rx/Tx LPI Status	リンク パートナーの低電力アイドル（LPI）ステータス。このフィールドには、次のいずれかの値を使用できます。 • N/A：ポートは EEE に対応できません。 • Interrupted：リンク パートナーは低電力モードへの移行中です。 • Low Power：リンク パートナーは低電力モードにあります。 • None：EEE がディセーブルであるか、リンク パートナー側で対応できません。 • Received：リンク パートナーは低電力モードにあり、トラフィック アクティビティがあります。 インターフェイスが半二重として設定されており、LPI ステータスが「None」の場合、インターフェイスが全二重として設定されるまで、インターフェイスは低電力モードにすることはできないことを意味します。
Wake Error Count	発生した PHY wake-up エラーの数EEE がイネーブルで、リンク パートナーへの接続が切断された場合に、wake-up エラーが発生します。 この情報は、PHY のデバッグに役立ちます。

show env

ファン、温度、、および電源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**| **fan**| **power** [**all**| **switch** [*stack-member-number*]]| **stack** [*stack-member-number*] | **temperature** [**status**]}

構文の説明

all	ファンと温度環境の状態、および、内部電源を表示します。
fan	スイッチのファンの状態を表示します。

power	アクティブ スイッチの内部電源の状態を表示します。
all	（任意）スイッチでコマンドが入力された場合、スタンドアロン スイッチのすべての内部電源の状態が表示されます。アクティブ スイッチでコマンドが入力された場合は、すべてのスタック メンバのすべての内部電源の状態が表示されます。
switch	（任意）スタック内の各スイッチまたは指定したスイッチの内部電源装置のステータスを表示します。 このキーワードは、スタック構成対応スイッチでだけ使用できます。
stack-member-number	（任意）内部電源または環境ステータスの状態を表示するスタック メンバの数。 指定できる範囲は 1 ～ 9 です。
stack	スタックの各スイッチまたは指定されたスイッチのすべての環境ステータスを表示します。 このキーワードは、スタック構成対応スイッチでだけ使用できます。
temperature	スイッチの温度ステータスを表示します。
status	（任意）スイッチの内部温度（外部温度ではなく）およびしきい値を表示します。

コマンド デフォルト

なし

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

アクセスされているスイッチ（スタンドアロンスイッチまたはアクティブスイッチ）の情報を表示するには、**show env** EXEC コマンドを使用します。**stack** および **switch** キーワードとともにこのコマンドを使用すると、スタックまたは指定されたスタック メンバのすべての情報が表示されます。

show env temperature status コマンドを入力すると、コマンド出力にスイッチの温度状態としきい値レベルが表示されます。

show env temperature コマンドを使用して、スイッチの温度状態を表示することもできます。コマンド出力では、GREEN および YELLOW ステートを *OK* と表示し、RED ステートを *FAULTY* と表示します。**show env all** コマンドを入力した場合のコマンド出力は、**show env temperature status** コマンド出力と同じです。

次に、**show env all** コマンドの出力例を示します。

```
Device>show env all
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

次に、**show env fan** コマンドの出力例を示します。

```
Device>show env fan
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
```

次に、**show env power** コマンドの出力例を示します。

```
Device>show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

次に、アクティブ スイッチ上での **show env power all** コマンドの出力例を示します。

```
Device# show env power all
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

次に、アクティブ スイッチ上での**show env stack** コマンドの出力例を示します。

```
Device> show env stack
SWITCH: 1
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
```

```
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
Temperature Value: 28 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold    : 56 Degree Celsius
```

次の例では、スタンドアロン スイッチで温度値、ステート、およびしきい値を表示する方法を示します。表に、コマンド出力での温度ステートの説明を示します。

```
Device> show env temperature status
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 65 Degree Celsius
Red Threshold    : 75 Degree Celsius
```

表 *16* : ***show env temperature status*** コマンド出力のステート

ステート	説明
Green	スイッチの温度が正常な動作範囲にあります。
Yellow	温度が警告範囲にあります。スイッチの外の周辺温度を確認する必要があります。
Red	温度がクリティカル範囲にあります。温度がこの範囲にある場合、スイッチが正常に実行されない可能性があります。

show errdisable detect

error-disabled 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。

コマンド デフォルト

なし

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

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。

コマンド出力内の errdisable の理由がアルファベット順に表示されます。Mode 列は、errdisable が機能ごとにどのように設定されているかを示します。

errdisable 検出は次のモードで設定できます。

- ポート モード：違反が発生した場合、物理ポート全体が errdisable になります。
- VLAN モード：違反が発生した場合、VLAN が errdisable になります。
- ポート/VLAN モード：一部のポートでは物理ポート全体が errdisable になり、その他のポートでは VLAN ごとに errdisable になります。

次の例では、**show errdisable detect** コマンドの出力を示します。

```
Device> show errdisable detect
ErrDisable Reason    Detection    Mode
-----------------    ---------    ----
arp-inspection       Enabled      port
bpduguard            Enabled      vlan
channel-misconfig    Enabled      port
community-limit      Enabled      port
dhcp-rate-limit      Enabled      port
dtp-flap             Enabled      port
gbic-invalid         Enabled      port
inline-power         Enabled      port
invalid-policy       Enabled      port
l2ptguard            Enabled      port
link-flap            Enabled      port
loopback             Enabled      port
lsgroup              Enabled      port
pagp-flap            Enabled      port
psecure-violation    Enabled      port/vlan
security-violatio    Enabled      port
sfp-config-mismat    Enabled      port
storm-control        Enabled      port
udld                 Enabled      port
vmps                 Enabled      port
```

関連トピック

show errdisable recovery, （204 ページ）

show errdisable recovery

error-disabled 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。

コマンド デフォルト

なし

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

gbic-invalid error-disable の理由は、無効な Small Form-Factor Pluggable（SFP）インターフェイスを意味します。

（注） unicast-flood フィールドは、出力に表示はされますが無効です。

次の例では、**show errdisable recovery** コマンドの出力を示します。

```
Device> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Enabled
```

```
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback             Disabled
Timer interval:300 seconds
Interfaces that will be enabled at the next timeout:
Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi1/0/2        link-flap             279
```

関連トピック

errdisable recovery cause, （152 ページ）

errdisable recovery interval, （155 ページ）

show errdisable detect, （202 ページ）

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*]| **debounce**| **description**| **etherchannel**| **flowcontrol**| **pruning**| **stats**| **status** [**err-disabled**| **inactive**]| **trunk**]

構文の説明

interface-id	（任意）インターフェイスの ID です。有効なインターフェイスには、物理ポート（タイプ、スタック構成可能なスイッチのスタック メンバ、モジュール、およびポート番号を含む）やポート チャネルが含まれます。指定できるポート チャネルは 1 ～ 48 です。
vlan *vlan-id*	（任意）VLAN ID です。指定できる範囲は 1 ～ 4094 です。
accounting	（任意）インターフェイスのアカウント情報（アクティブ プロトコル、入出力のパケット、オクテットを含む）を表示します。 （注） ソフトウェアで処理されたパケットだけが表示されます。ハードウェアでスイッチングされるパケットは表示されません。
capabilities	（任意）すべてのインターフェイスまたは指定されたインターフェイスの性能（機能、インターフェイス上で設定可能なオプションを含む）を表示します。このオプションはコマンドラインのヘルプに表示されますが、VLAN ID に使用できません。

module *number*	（任意）スイッチまたは指定されたスタック メンバーのすべてのインターフェイスの機能を表示します。 指定できる範囲は 1 ～ 9 です。 このオプションは、特定のインターフェイス ID を入力したときは利用できません。
debounce	（任意）インターフェイスのポートデバウンス タイマー情報を表示します。
description	（任意）特定のインターフェイスに設定された管理ステータスおよび説明を表示します。
etherchannel	（任意）インターフェイス EtherChannel 情報を表示します。
flowcontrol	（任意）インターフェイスのフロー制御情報を表示します。
mtu	（任意）各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応する MTU を表示します。
pruning	（任意）インターフェイスのトランク VTP プルーニング情報を表示します。
stats	（任意）インターフェイスのパスを切り替えることによる入出力パケットを表示します。
status	（任意）インターフェイスのステータスを表示します。Type フィールドの unsupported のステータスは、他社製の Small Form-Factor Pluggable（SFP）モジュールがモジュール スロットに装着されていることを示しています。
err-disabled	（任意）errdisable ステートのインターフェイスを表示します。
inactive	（任意）非アクティブ ステートのインターフェイスを表示します。
trunk	（任意）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。

（注） **crb**、**fair-queue**、**irb**、**mac-accounting**、**precedence**、**random-detect**、および **rate-limit** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

コマンド モード 特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

- **show interface capabilities module** *number* コマンドを使用して、スタックのスイッチ上のすべてのインターフェイスの機能を表示します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。
- 指定されたインターフェイスの機能を表示するには、**show interfaces** *interface-id* **capabilities** を使用します。
- スタック内のすべてのインターフェイスの機能を表示するには、**show interfaces capabilities** を使用します（モジュール番号またはインターフェイス ID の指定なし）。

次の例では、スタック メンバ 3 のインターフェイスに対する **show interfaces** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, 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 never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     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。

次の例では、インターフェイスに対する **show interfaces capabilities** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model:                 UA-3850-24-CR
  Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                full,half,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  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
```

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。

```
Device# show interfaces gigabitethernet1/0/2 description
Interface                      Status         Protocol Description
Gi1/0/2                        up             down     Connects to Marketing
```

次の例では、スイッチにポート チャネルが設定されている場合の **show interfaces etherchannel** コマンドの出力を示します。

```
Device# show interfaces etherchannel
-----
Port-channel34:
Age of the Port-channel   = 28d:18h:51m:46s
Logical slot/port   = 12/34          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Passive port list   =
Port state          = Port-channel L3-Ag Ag-Not-Inuse
Protocol            =    -
Port security       = Disabled
```

次の例では、VTP ドメイン内でプルーニングがイネーブルの場合の **show interfaces** *interface-id* **pruning** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

次の例では、指定した VLAN インターフェイスの **show interfaces stats** コマンドの出力を示します。

```
Device# 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。

次の例では、**show interfaces***interface-id***status** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet1/0/20 status
Port      Name               Status       Vlan       Duplex  Speed       Type
Gi1/0/20                     notconnect   1            auto   auto 10/100/1000Ba
seTX
```

次の例では、**show interfaces status err-disabled** コマンドの出力を示します。errdisable ステートのインターフェイスのステータスを表示します。

```
Device# show interfaces status err-disabled
Port      Name       Status         Reason
Gi1/0/2              err-disabled   gbic-invalid
Gi2/0/3              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。

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

次の例では、**show interfaces** *interface-id* **trunk** コマンドの出力を示します。ポートのトランキング情報が表示されます。

```
Device# show interfaces gigabitethernet1/0/1 trunk
Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/1     on               802.1q         other         10

Port        Vlans allowed on trunk
Gi1/0/1     none

Port        Vlans allowed and active in management domain
Gi1/0/1     none

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/1     none
```

関連トピック

show interfaces counters, （209 ページ）

show interfaces switchport, （212 ページ）

show interfaces transceiver, （214 ページ）

show interfaces counters

スイッチまたは特定のインターフェイスのさまざまな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*] **counters** [**errors**| **etherchannel**| **module** *stack-member-number*| **protocol status**| **trunk**]

構文の説明

interface-id	（任意）物理インターフェイスの ID（タイプ、スタック メンバ（スタック構成可能なスイッチのみ）、モジュール、ポート番号を含む）。
errors	（任意）エラー カウンタを表示します。

etherchannel	（任意）送受信されたオクテット、ブロードキャスト パケット、マルチキャスト パケット、およびユニキャスト パケットなど、EtherChannel カウンタを表示します。
module *stack-member-number*	（任意）指定されたスタック メンバのカウンタを表示します。 指定できる範囲は 1 ～ 9 です。 （注） このコマンドでは、**module** キーワードはスタック メンバ番号を参照しています。インターフェイス ID に含まれるモジュール番号は、常に 0 です。
protocol status	（任意）インターフェイスでイネーブルになっているプロトコルのステータスを表示します。
trunk	（任意）トランク カウンタを表示します。

（注） **vlan** *vlan-id* キーワードは、コマンドラインのヘルプ文字列には表示されますが、サポートされていません。

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
Cisco IOS XE 3.2SE	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。

次の例では、**show interfaces counters** コマンドの出力の一部を示します。スイッチのすべてのカウンタが表示されます。

```
Device# show interfaces counters
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1                0              0              0              0
```

```
Gi1/0/2                 0              0              0              0
Gi1/0/3          95285341          43115        1178430           1950
Gi1/0/4                 0              0              0              0

<output truncated>
```

次の例では、スタック メンバ 2 に対する **show interfaces counters module** コマンドの出力の一部を示します。スタック内で指定されたスイッチのすべてのカウンタが表示されます。

```
Device# show interfaces counters module 2
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1              520              2              0              0
Gi1/0/2              520              2              0              0
Gi1/0/3              520              2              0              0
Gi1/0/4              520              2              0              0

<output truncated>
```

次の例では、すべてのインターフェイスに対する **show interfaces counters protocol status** コマンドの出力の一部を示します。

```
Device# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP

<output truncated>
```

次の例では、**show interfaces counters trunk** コマンドの出力を示します。すべてのインターフェイスのトランク カウンタが表示されます。

```
Device# show interfaces counters trunk
Port        TrunkFramesTx   TrunkFramesRx   WrongEncap
Gi1/0/1                 0               0            0
Gi1/0/2                 0               0            0
Gi1/0/3             80678               0            0
Gi1/0/4             82320               0            0
Gi1/0/5                 0               0            0

<output truncated>
```

関連トピック

show interfaces, （205 ページ）

show interfaces switchport

ポート ブロッキング、ポート保護設定など、スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示するには、特権 EXEC モードで **show interfaces switchport** コマンドを使用します。

show interfaces [*interface-id*] **switchport** [**module** *number*]

構文の説明

interface-id	（任意）インターフェイスのIDです。有効なインターフェイスには、物理ポート（タイプ、スタック構成可能なスイッチのスタック メンバ、モジュール、およびポート番号を含む）やポート チャネルが含まれます。指定できるポート チャネルは 1 ～ 48 です。
module *number*	（任意）スイッチまたは指定されたスタック メンバのすべてのインターフェイスのスイッチポート設定を表示します。 指定できる範囲は 1 ～ 9 です。 このオプションは、特定のインターフェイス ID を入力したときは利用できません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

スタックのスイッチ上のすべてのインターフェイスのスイッチ ポート特性を表示するには、**show interface switchport module** *number* コマンドを使用します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。

次の例では、ポートの **show interfaces switchport** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

（注） プライベート VLAN はこのリリースではサポートされないので、フィールドは適用されません。

```
Device# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

フィールド	説明
Name	ポート名を表示します。
Switchport	ポートの管理ステータスおよび動作ステータスを表示します。この出力の場合、ポートはスイッチポート モードです。
Administrative Mode Operational Mode	管理モードおよび動作モードを表示します。
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	管理上および運用上のカプセル化方式、およびトランキング ネゴシエーションがイネーブルかどうかを表示します。
Access Mode VLAN	ポートを設定する VLAN ID を表示します。

フィールド	説明
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	ネイティブ モードのトランクの VLAN ID を一覧表示します。トランク上の許可VLANを一覧表示します。トランク上のアクティブVLANを一覧表示します。
Pruning VLANs Enabled	プルーニングに適格な VLAN を一覧表示します。
Protected	インターフェイス上で保護ポートがイネーブル（True）であるかまたはディセーブル（False）であるかを表示します。
Unknown unicast blocked Unknown multicast blocked	不明なマルチキャストおよび不明なユニキャストトラフィックがインターフェイス上でブロックされているかどうかを表示します。
Voice VLAN	音声 VLAN がイネーブルである VLAN ID を表示します。
Appliance trust	IP Phone のデータ パケットのサービス クラス（CoS）設定を表示します。

関連トピック

show interfaces, （205 ページ）

show interfaces transceiver

SFP モジュール インターフェイスの物理インターフェイスを表示するには、EXEC モードで **show interfaces transceiver** コマンドを使用します。

show interfaces [*interface-id*] **transceiver** [**detail**| **module** *number*| **properties**| **supported-list**| **threshold-table**]

構文の説明

interface-id	（任意）物理インターフェイスの ID（タイプ、スタック メンバ（スタック構成可能なスイッチのみ）、モジュール、ポート番号を含む）。
detail	（任意）（スイッチにインストールされている場合）Digital Optical Monitoring（DoM）対応トランシーバの高低値やアラーム情報などの、調整プロパティを表示します。

module*number*	（任意）スイッチのモジュールのインターフェイスへの表示を制限します。 指定できる範囲は 1 ～ 9 です。 このオプションは、特定のインターフェイス ID を入力したときは利用できません。
properties	（任意）インターフェイスの速度、デュプレックス、およびインラインパワー設定を表示します。
supported-list	（任意）サポートされるトランシーバをすべて表示します。
threshold-table	（任意）アラームおよび警告しきい値テーブルを表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show interfaces** *interface-id* **transceiver properties** コマンドの出力例を示します。

```
Device# show interfaces gigabitethernet1/1/1 transceiver properties
  Name : Gi1/1/1
  Administrative Speed: auto
  Operational Speed: auto
  Administrative Duplex: auto
  Administrative Power Inline: enable
  Operational Duplex: auto
  Administrative Auto-MDIX: off
  Operational Auto-MDIX: off
```

次に、**show interfaces** *interface-id* **transceiver detail** コマンドの出力例を示します。

```
Device# show interfaces gigabitethernet1/1/1 transceiver detail
  ITU Channel not available (Wavelength not available),
  Transceiver is internally calibrated.
  mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
  ++:high alarm, +:high warning, -:low warning, -- :low alarm.
  A2D readouts (if they differ), are reported in parentheses.
  The threshold values are uncalibrated.

                              High Alarm  High Warn  Low Warn   Low Alarm
           Temperature        Threshold   Threshold  Threshold  Threshold
  Port     (Celsius)         (Celsius)   (Celsius)  (Celsius)  (Celsius)
  -------  -----------------  ----------  ---------  ---------  ---------
```

```
Gi1/1/1  29.9                74.0         70.0         0.0          -4.0
                             High Alarm   High Warn    Low Warn     Low Alarm
         Voltage             Threshold    Threshold    Threshold    Threshold
Port     (Volts)             (Volts)      (Volts)      (Volts)      (Volts)
-------  ----------------    ----------   ---------    ---------    ---------
Gi1/1/1  3.28                3.60         3.50         3.10         3.00

         Optical             High Alarm   High Warn    Low Warn     Low Alarm
         Transmit Power      Threshold    Threshold    Threshold    Threshold
Port     (dBm)               (dBm)        (dBm)        (dBm)        (dBm)
-------  ------------------  ----------   ---------    ---------    ---------
Gi1/1/1  1.8                 7.9          3.9          0.0          -4.0

         Optical             High Alarm   High Warn    Low Warn     Low Alarm
         Receive Power       Threshold    Threshold    Threshold    Threshold
Port     (dBm)               (dBm)        (dBm)        (dBm)        (dBm)
-------  ------------------  ----------   ---------    ---------    ---------
Gi1/1/1  -23.5               -5.0         -9.0         -28.2        -32.2
```

次に、**show interfaces transceiver threshold-table** コマンドの出力例を示します。

```
Device# show interfaces transceiver threshold-table
              Optical Tx     Optical Rx    Temp      Laser Bias     Voltage
                                                     current
             -------------  -------------  ------   ------------  ---------

 DWDM GBIC
Min1              -4.00        -32.00        -4           N/A          4.65
Min2               0.00        -28.00         0           N/A          4.75
Max2               4.00         -9.00        70           N/A          5.25
Max1               7.00         -5.00        74           N/A          5.40
 DWDM SFP
Min1              -4.00        -32.00        -4           N/A          3.00
Min2               0.00        -28.00         0           N/A          3.10
Max2               4.00         -9.00        70           N/A          3.50
Max1               8.00         -5.00        74           N/A          3.60
 RX only WDM GBIC
Min1               N/A          -32.00        -4           N/A          4.65
Min2               N/A          -28.30         0           N/A          4.75
Max2               N/A           -9.00        70           N/A          5.25
Max1               N/A           -5.00        74           N/A          5.40
 DWDM XENPAK
Min1              -5.00        -28.00        -4           N/A          N/A
Min2              -1.00        -24.00         0           N/A          N/A
Max2               3.00         -7.00        70           N/A          N/A
Max1               7.00         -3.00        74           N/A          N/A
 DWDM X2
Min1              -5.00        -28.00        -4           N/A          N/A
Min2              -1.00        -24.00         0           N/A          N/A
Max2               3.00         -7.00        70           N/A          N/A
Max1               7.00         -3.00        74           N/A          N/A
 DWDM XFP
Min1              -5.00        -28.00        -4           N/A          N/A
Min2              -1.00        -24.00         0           N/A          N/A
Max2               3.00         -7.00        70           N/A          N/A
Max1               7.00         -3.00        74           N/A          N/A
 CWDM X2
Min1               N/A           N/A          0           N/A          N/A
Min2               N/A           N/A          0           N/A          N/A
Max2               N/A           N/A          0           N/A          N/A
Max1               N/A           N/A          0           N/A          N/A

<output truncated>
```

関連トピック

show interfaces, （205 ページ）

show memory platform

プラットフォームのメモリ統計情報を表示するには、特権 EXEC モードで **show memory platform** コマンドを使用します。

show memory platform [**compressed-swap**| **information**| **page-merging**]

構文の説明

compressed-swap	（任意）プラットフォーム メモリの圧縮スワップ情報を表示します。
information	（任意）プラットフォームに関する一般的な情報を表示します。
page-merging	（任意）プラットフォーム メモリのページマージング情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

Cisco IOS XE Denali 16.3.1 より前は、コマンド出力に表示される「空きメモリ」は基盤となる Linux カーネルから得ていました。使用可能な一部のメモリ チャンクは空きメモリと見なされていなかったため、この値は正確ではありませんでした。

Cisco IOS XE Denali 16.3.1 では、空きメモリは正確に計算されて、コマンド出力の Free Memory フィールドに表示されます。

次に、**show memory platform** コマンドの出力例を示します。

```
Switch# show memory platform

 Virtual memory   : 12874653696
  Pages resident   : 627041
  Major page faults: 2220
  Minor page faults: 2348631

  Architecture     : mips64
  Memory (kB)
    Physical       : 3976852
    Total          : 3976852
    Used           : 2761276
```

```
    Free           : 1215576
    Active         : 2128196
    Inactive       : 1581856
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 0
    AnonPages      : 1294984
    Bounce         : 0
    Cached         : 1978168
    Commit Limit   : 1988424
    Committed As   : 3343324
    High Total     : 0
    High Free      : 0
    Low Total      : 3976852
    Low Free       : 1215576
    Mapped         : 516316
    NFS Unstable   : 0
    Page Tables    : 17124
    Slab           : 0
    VMmalloc Chunk : 1069542588
    VMmalloc Total : 1069547512
    VMmalloc Used  : 2588
    Writeback      : 0
    HugePages Total: 0
    HugePages Free : 0
    HugePages Rsvd : 0
    HugePage Size  : 2048

  Swap (kB)
    Total          : 0
    Used           : 0
    Free           : 0
    Cached         : 0

  Buffers (kB)     : 437136

  Load Average
    1-Min          : 1.04
    5-Min          : 1.16
    15-Min         : 0.94
```

次に、**show memory platform information** コマンドの出力例を示します。

```
Device# show memory platform information

 Virtual memory   : 12870438912
  Pages resident   : 626833
  Major page faults: 2222
  Minor page faults: 2362455

  Architecture     : mips64
  Memory (kB)
    Physical       : 3976852
    Total          : 3976852
    Used           : 2761224
    Free           : 1215628
    Active         : 2128060
    Inactive       : 1584444
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 284
    AnonPages      : 1294656
    Bounce         : 0
    Cached         : 1979644
    Commit Limit   : 1988424
    Committed As   : 3342184
    High Total     : 0
    High Free      : 0
    Low Total      : 3976852
    Low Free       : 1215628
    Mapped         : 516212
    NFS Unstable   : 0
```

```
  Page Tables    : 17096
  Slab           : 0
  VMmalloc Chunk : 1069542588
  VMmalloc Total : 1069547512
  VMmalloc Used  : 2588
  Writeback      : 0
  HugePages Total: 0
  HugePages Free : 0
  HugePages Rsvd : 0
  HugePage Size  : 2048

Swap (kB)
  Total          : 0
  Used           : 0
  Free           : 0
  Cached         : 0

Buffers (kB)     : 438228

Load Average
  1-Min          : 1.54
  5-Min          : 1.27
  15-Min         : 0.99
```

show module

スイッチ番号、モデル番号、シリアル番号、ハードウェア リビジョン番号、ソフトウェア バージョン、MAC アドレスなどのモジュール情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで、このコマンドを使用します。

show module [*switch-num*]

構文の説明

switch-num	（任意）スイッチの番号。

コマンド デフォルト

なし

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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

switch-num 引数を指定せずに **show module** コマンドを入力した場合、show module all コマンドを入力した場合と同じ結果になります。

次に、Cisco Catalyst 3850 シリーズ スイッチ上のすべてのモジュールの情報を表示する例を示します。

show mgmt-infra trace messages ilpower

トレース バッファ内のインライン パワーのメッセージを表示するには、特権 EXEC モードで **show mgmt-infra trace messages ilpower** コマンドを使用します。

show mgmt-infra trace messages ilpower [**switch** *stack-member-number*]

構文の説明

switch *stack-member-number*	（任意）トレース バッファ内のインライン パワーのメッセージを表示するスタック メンバ番号を指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show mgmt-infra trace messages ilpower** コマンドの出力例を示します。

```
Device# show mgmt-infra trace messages ilpower
[10/23/12 14:05:10.984 UTC 1 3] Initialized inline power system configuration fo
r slot 1.
[10/23/12 14:05:10.984 UTC 2 3] Initialized inline power system configuration fo
r slot 2.
[10/23/12 14:05:10.984 UTC 3 3] Initialized inline power system configuration fo
r slot 3.
[10/23/12 14:05:10.984 UTC 4 3] Initialized inline power system configuration fo
r slot 4.
[10/23/12 14:05:10.984 UTC 5 3] Initialized inline power system configuration fo
r slot 5.
```

```
[10/23/12 14:05:10.984 UTC 6 3] Initialized inline power system configuration fo
r slot 6.
[10/23/12 14:05:10.984 UTC 7 3] Initialized inline power system configuration fo
r slot 7.
[10/23/12 14:05:10.984 UTC 8 3] Initialized inline power system configuration fo
r slot 8.
[10/23/12 14:05:10.984 UTC 9 3] Initialized inline power system configuration fo
r slot 9.
[10/23/12 14:05:10.984 UTC a 3] Inline power subsystem initialized.
[10/23/12 14:05:18.908 UTC b 264] Create new power pool for slot 1
[10/23/12 14:05:18.909 UTC c 264] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.273 UTC d 3] PoE is not supported on .
[10/23/12 14:05:20.288 UTC e 3] PoE is not supported on .
[10/23/12 14:05:20.299 UTC f 3] PoE is not supported on .
[10/23/12 14:05:20.311 UTC 10 3] PoE is not supported on .
[10/23/12 14:05:20.373 UTC 11 98] Inline power process post for switch 1
[10/23/12 14:05:20.373 UTC 12 98] PoE post passed on switch 1
[10/23/12 14:05:20.379 UTC 13 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:20.379 UTC 14 3] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.379 UTC 15 3] Gi1/0/1 port config Initialized
[10/23/12 14:05:20.379 UTC 16 3] Interface Gi1/0/1 initialization done.
[10/23/12 14:05:20.380 UTC 17 3] Gi1/0/24 port config Initialized
[10/23/12 14:05:20.380 UTC 18 3] Interface Gi1/0/24 initialization done.
[10/23/12 14:05:20.380 UTC 19 3] Slot #1: initialization done.
[10/23/12 14:05:50.440 UTC 1a 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:50.440 UTC 1b 3] Duplicate init event
```

show mgmt-infra trace messages ilpower-ha

トレースバッファ内のインラインパワーのハイアベイラビリティのメッセージを表示するには、特権 EXEC モードで **show mgmt-infra trace messages ilpower-ha** コマンドを使用します。

show mgmt-infra trace messages ilpower-ha [**switch** *stack-member-number*]

構文の説明

switch *stack-member-number*	（任意）トレース バッファ内のインライン パワーのメッセージを表示するスタック メンバ番号を指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show mgmt-infra trace messages ilpower-ha** コマンドの出力例を示します。

```
Device# show mgmt-infra trace messages ilpower-ha
[10/23/12 14:04:48.087 UTC 1 3] NG3K_ILPOWER_HA: Created NGWC ILP CF client succ
essfully.
```

show mgmt-infra trace messages platform-mgr-poe

トレース バッファ内のプラットフォーム マネージャの Power over Ethernet（PoE）メッセージを表示するには、**show mgmt-infra trace messages platform-mgr-poe** 特権 EXEC コマンドを使用します。

show mgmt-infra trace messages platform-mgr-poe [**switch** *stack-member-number*]

構文の説明

switch *stack-member-number*	（任意）トレース バッファ内のメッセージを表示するスタック メンバ番号を指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show mgmt-infra trace messages platform-mgr-poe** コマンドの一部の出力例を示します。

```
Device# show mgmt-infra trace messages platform-mgr-poe
[10/23/12 14:04:06.431 UTC 1 5495] PoE Info: get power controller param sent:
[10/23/12 14:04:06.431 UTC 2 5495] PoE Info: POE_SHUT sent for port 1 (0:0)
[10/23/12 14:04:06.431 UTC 3 5495] PoE Info: POE_SHUT sent for port 2 (0:1)
[10/23/12 14:04:06.431 UTC 4 5495] PoE Info: POE_SHUT sent for port 3 (0:2)
[10/23/12 14:04:06.431 UTC 5 5495] PoE Info: POE_SHUT sent for port 4 (0:3)
[10/23/12 14:04:06.431 UTC 6 5495] PoE Info: POE_SHUT sent for port 5 (0:4)
[10/23/12 14:04:06.431 UTC 7 5495] PoE Info: POE_SHUT sent for port 6 (0:5)
[10/23/12 14:04:06.431 UTC 8 5495] PoE Info: POE_SHUT sent for port 7 (0:6)
[10/23/12 14:04:06.431 UTC 9 5495] PoE Info: POE_SHUT sent for port 8 (0:7)
[10/23/12 14:04:06.431 UTC a 5495] PoE Info: POE_SHUT sent for port 9 (0:8)
[10/23/12 14:04:06.431 UTC b 5495] PoE Info: POE_SHUT sent for port 10 (0:9)
[10/23/12 14:04:06.431 UTC c 5495] PoE Info: POE_SHUT sent for port 11 (0:10)
[10/23/12 14:04:06.431 UTC d 5495] PoE Info: POE_SHUT sent for port 12 (0:11)
[10/23/12 14:04:06.431 UTC e 5495] PoE Info: POE_SHUT sent for port 13 (e:0)
```

```
[10/23/12 14:04:06.431 UTC f 5495] PoE Info: POE_SHUT sent for port 14 (e:1)
[10/23/12 14:04:06.431 UTC 10 5495] PoE Info: POE_SHUT sent for port 15 (e:2)
[10/23/12 14:04:06.431 UTC 11 5495] PoE Info: POE_SHUT sent for port 16 (e:3)
[10/23/12 14:04:06.431 UTC 12 5495] PoE Info: POE_SHUT sent for port 17 (e:4)
[10/23/12 14:04:06.431 UTC 13 5495] PoE Info: POE_SHUT sent for port 18 (e:5)
[10/23/12 14:04:06.431 UTC 14 5495] PoE Info: POE_SHUT sent for port 19 (e:6)
[10/23/12 14:04:06.431 UTC 15 5495] PoE Info: POE_SHUT sent for port 20 (e:7)
[10/23/12 14:04:06.431 UTC 16 5495] PoE Info: POE_SHUT sent for port 21 (e:8)
[10/23/12 14:04:06.431 UTC 17 5495] PoE Info: POE_SHUT sent for port 22 (e:9)
[10/23/12 14:04:06.431 UTC 18 5495] PoE Info: POE_SHUT sent for port 23 (e:10)
```

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*]

構文の説明

profile-number	（任意）ネットワークポリシープロファイル番号を表示します。プロファイルが入力されていない場合、すべてのネットワーク ポリシープロファイルが表示されます。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show network-policy profile** コマンドの出力を示します。

```
Device# show network-policy profile
Network Policy Profile 60
  Interface:
   none
```

関連トピック

network-policy, （167 ページ）

network-policy profile（グローバル コンフィギュレーション）, （168 ページ）

show platform CAPWAP summary

アクセスポイントとその他のモビリティコントローラに対してコントローラが確立するすべてのCAPWAP トンネルのトンネル識別子およびタイプを表示するには、**show platform CAPWAP summary** コマンドを使用します。

show platform CAPWAP summary

構文の説明

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、トンネルの識別子と詳細を表示する例を示します。

```
Device# show platform capwap summary
Tunnel ID | Type | Src IP | Dst IP | SPrt | DPrt | S | A
------------------------------------------------------------------------------

0x0088498000000983 data 9.6.44.61 9.12.138.101 5247 41894 1 1

0x00966dc000000010 data 9.6.44.61 9.6.47.101 5247 62526 1 2
0x00938e800000095b data 9.6.44.61 9.12.138.100 5247 45697 1 1

0x00ab1a8000000bd1 data 9.6.44.61 9.12.139.101 5247 38906 1 0

0x00896e40000000bd data 9.6.44.61 9.12.136.100 5247 1836 1 1
```

show platform forward

指定されたパラメータと一致したフレームがハードウェアで転送される方法を指定するには、インターフェイスに対して **show platform forward** 特権 EXEC コマンドを使用します。

show platform forward*interface-id* [**vlan** *vlan-id*] *src-macdst-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-post dst-port flags* | **udp***src-port dst-port*] } [| { **begin** | **exclude** | **include** } *expression*]

構文の説明

interface-id	パケットがスイッチに着信するポートとなる入力物理インターフェイス（タイプ、ポート番号を含む）。
vlan*vlan-id*	（任意）入力 VLAN ID。指定できる範囲は 1 ～ 4094 です。この値が指定されず、入力インターフェイスがルーテッドポートでない場合、デフォルトは 1 です。
src-mac	48 ビット送信元 MAC アドレス。
dst-mac	48 ビット宛先 MAC アドレス。
ipv6	（任意）IPv6 フレーム。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のみ使用できます。
sap	（任意）サービス アクセス ポイント（SAP）カプセル化タイプ
snap	（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
cos*cos*	（任意）フレームのサービス クラス（CoS）値。指定できる範囲は 0 ～ 7 です。
ip*src-ip dst-ip*	（任意、ただし IP パケットの場合は必須）ドット付き 10 進表記の送信元および宛先 IP アドレス。
frag*field*	（任意）フラグメント IP パケットの IP フラグメント フィールド。指定できる範囲は 0 ～ 65535 です。
dscp*dscp*	（任意）IP ヘッダーの Diffserv コードポイント（DSCP）フィールド。指定できる範囲は 0 ～ 63 です。
l4protocol-id	IP ヘッダーのレイヤ 4 プロトコル フィールドの数値。指定できる範囲は 0 ～ 255 です。たとえば、47 は総称ルーティング 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。
icmp*icmp-type icmp-code*	ICMP パラメータ。icmp-type および icmp-code に指定できる範囲は 0 ～ 255 です。
igmp *igmp-version igmp-type*	IGMP パラメータ。指定できる範囲は、*igmp-version* は 1 ～ 15、*igmp-type* は 0 ～ 15 です。

sctp*src-port dst-port*	Stream Control Transmission Protocol（SCTP）パラメータ。SCTP 送信元および宛先ポートに指定できる範囲は 0 ～ 65535 です。
tcp*src-post dst-port flags*	TCP パラメータ：TCP 送信元ポート、宛先ポート、ヘッダーの TCP フラグ バイトの数値。src-port および dst-port に指定できる範囲は 0 ～ 65535 です。指定できるフラグ範囲は 0 ～ 1024 です。
udp*src-port dst-port*	UDP パラメータ。src-port および dst-port に指定できる範囲は 0 ～ 65535 です。
| begin	（任意）*expression* と一致する行から表示を開始します。
| exclude	（任意）*expression* と一致する行を表示から除外します。
| include	（任意）指定された *expression* と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の文字列です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが再度導入されました。

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。

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

show platform hardware fed switch forward

デバイス固有のハードウェア情報を表示するには、**show platform hardware fed switch***switch_number* コマンドを使用します。

このトピックでは、転送特有のオプション、つまり **show platform hardware fed switch** {*switch_num* | **active** | **standby** }**forward summary** コマンドで使用可能なオプションのみについて詳しく説明します。

show platform hardware fed switch*switch_number***forward summary** の出力は、パケットに対して実行される転送の決定に関するすべての詳細を表示します。

show platform hardware fed switch{*switch_num*| **active**| **standby**} **forward summary**

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するスイッチ。次のオプションがあります。 • *switch_num*：スイッチの ID。 • **active**：アクティブ スイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイ スイッチに関する情報を表示します。
forward summary	パケット転送の情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

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。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。

コマンド出力に表示されるフィールドついて、以下で説明します。

- Station Index（ステーション インデックス）：Station Index は、レイヤ 2 ルックアップの結果で、以下を表示するステーション記述子にポイントします。
  - Destination Index（接続先インデックス）：パケットを送信する出力ポートを決定します。グローバル ポート番号（GPN）は、接続先インデックスとして使用できます。15 から 12 ビットの接続先インデックスのセットは、使用される GPN を示します。たとえば、接続先インデックス 0xF04E は GPN - 78（0x4e）に対応します。
  - Rewrite Index（書き換えインデックス）：パケットで何が実行される必要があるかを決定します。レイヤ 2 スイッチングの場合、通常はブリッジング アクションです。

- Flexible Lookup Pipeline Stages（FPS）（フレキシブル ルックアップ パイプライン ステージ）：パケットのルーティングまたはブリッジングのために下された転送判断を示します。
- Replication Bit Map（複製ビット マップ）：パケットを CPU またはスタックに送信する必要があるかどうかを決定します。
  - ローカル データ コピー = 1
  - リモート データ コピー = 0
  - ローカル CPU コピー = 0
  - リモート CPU コピー = 0

例

これは、**show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward summary** コマンドの出力例です。

```
Device#show platform hardware fed switch 1 forward summary
Time: Fri Sep 16 08:25:00 PDT 2016

Incomming Packet Details:

###[ Ethernet ]###
  dst       = 00:51:0f:f2:0e:11
  src       = 00:1d:01:85:ba:22
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = 6
     plen      = 4
     op        = is-at
     hwsrc     = 00:1d:01:85:ba:22
     psrc      = 10.10.1.33
     hwdst     = 00:51:0f:f2:0e:11
     pdst      = 10.10.1.1

Ingress:
Switch             : 1
Port               : GigabitEthernet1/0/1
Global Port Number : 1
Local Port Number  : 1
Asic Port Number   : 21
ASIC Number        : 0
STP state          :
                     blkLrn31to0: 0xffdfffdf
                     blkFwd31to0: 0xffdfffdf
Vlan               : 1
Station Descriptor : 170
DestIndex          : 0xF009
DestModIndex       : 2
RewriteIndex       : 2
Forwarding Decision: FPS 2A L2 Destination

Replication Bitmap:
Local CPU copy     : 0
Local Data copy    : 1
Remote CPU copy    : 0
Remote Data copy   : 0

Egress:
```

```
Switch             : 1
Outgoing Port      : GigabitEthernet1/0/9
Global Port Number : 9
ASIC Number        : 0
Vlan               : 1
```

show platform resources

プラットフォームのリソース情報を表示するには、特権 EXEC モードで **show platform reources** コマンドを使用します。

show platform resources

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	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は、総メモリから正確な空きメモリを引いた値である使用メモリが表示されます。

例

次に、**show platform resources** コマンドの出力例を示します。

```
Switch# show platform resources

**State Acronym: H - Healthy, W - Warning, C - Critical

Resource                Usage                Max             Warning         Critical
     State
------------------------------------------------------------------------------------------------

 Control Processor      7.20%                100%            90%             95%
     H
  DRAM                  2701MB(69%)          3883MB          90%             95%
     H
```

show platform software ilpower

デバイス上のすべての PoE ポートのインライン パワーの詳細を表示するには、特権 EXEC モードで **showplatformsoftwareilpower** コマンドを使用します。

show platform software ilpower {**details** | **port** {**GigabitEthernet***interface-number* } | **system***slot-number* }

構文の説明

details	すべてのインターフェイスのインライン パワーの詳細を表示します。
port	インライン パワー ポートの設定を表示します。
GigabitEthernet*interface-number*	GigabitEthernet インターフェイス番号。値の範囲は 0 ～ 9 です。
system*slot-number*	インライン パワー システムの設定を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが変更されました。キーワード **details** 引数が追加されました。
Cisco IOS XE Denali 16.1.1	このコマンドが追加されました。

例

次に、**showplatformsoftwareilpowerdetails** コマンドの出力例を示します。

```
Device# show platform software ilpower details
ILP Port Configuration for interface Gi1/0/1
    Initialization Done:   Yes
    ILP Supported:         Yes
    ILP Enabled:           Yes
    POST:                  Yes
    Detect On:             No
    Powered Device Detected            No
    Powered Device Class Done          No
    Cisco Powered Device:              No
    Power is On:           No
    Power Denied:          No
    Powered Device Type:               Null
    Powerd Device Class:              Null
    Power State:           NULL
    Current State:         NGWC_ILP_DETECTING_S
    Previous State:        NGWC_ILP_SHUT_OFF_S
    Requested Power in milli watts:       0
    Short Circuit Detected:                 0
    Short Circuit Count:             0
    Cisco Powerd Device Detect Count: 0
```

```
Spare Pair mode:       0
    IEEE Detect:       Stopped
    IEEE Short:        Stopped
    Link Down:         Stopped
    Voltage sense:            Stopped
Spare Pair Architecture:       1
Signal Pair Power allocation in milli watts: 0
Spare Pair Power On:   0
Powered Device power state:        0
Timer:
    Power Good:        Stopped
    Power Denied:      Stopped
    Cisco Powered Device Detect:   Stopped
```

show platform software process list

プラットフォームで実行中のプロセスのリストを表示するには、特権EXECモードで**show platform software process list** コマンドを使用します。

show platform software process list switch {*switch-number*| **active**| **standby**} {**0**| **F0**| **R0**} [**name***process-name*| **process-id***process-ID*| **sortmemory**| **summary**]

構文の説明

switch*switch-number*	スイッチに関する情報を表示します。*switch-number* 引数の有効な値は 0 ～ 9 です。
active	スイッチのアクティブ インスタンスに関する情報を表示します。
standby	スイッチのスタンバイ インスタンスに関する情報を表示します。
0	共有ポート アダプタ（SPA）インターフェイス プロセッサ スロット 0 に関する情報を表示します。
F0	Embedded Service Processor（ESP）スロット 0 に関する情報を表示します。
R0	ルート プロセッサ（RP）スロット 0 に関する情報を表示します。
name*process-name*	（任意）指定されたプロセスに関する情報を表示します。
process-id*process-ID*	（任意）指定されたプロセス ID に関する情報を表示します。
sort	（任意）プロセスに従いソートされた情報を表示します。
memory	（任意）メモリに従いソートされた情報を表示します。
summary	（任意）ホスト デバイスのプロセス メモリのサマリーを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	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 XE Denali 16.3.1 より前は、コマンド出力に表示される「空きメモリ」は基盤となる Linux カーネルから得ていました。使用可能な一部のメモリ チャンクは空きメモリと見なされていなかったため、この値は正確ではありませんでした。

Cisco IOS XE Denali 16.3.1 では、空きメモリは正確に計算されて、コマンド出力の Free Memory フィールドに表示されます。

次に、**show platform software process list switch active R0** コマンドの出力例を示します。

```
Switch# show platform software process list switch active R0 summary

Total number of processes: 278
  Running          : 2
  Sleeping         : 276
  Disk sleeping    : 0
  Zombies          : 0
  Stopped          : 0
  Paging           : 0

  Up time          : 8318
  Idle time        : 0
  User time        : 216809
  Kernel time      : 78931

  Virtual memory   : 12933324800
  Pages resident   : 634061
  Major page faults: 2228
  Minor page faults: 3491744

  Architecture     : mips64
  Memory (kB)
    Physical       : 3976852
    Total          : 3976852
    Used           : 2766952
    Free           : 1209900
    Active         : 2141344
    Inactive       : 1589672
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 4
    AnonPages      : 1306800
    Bounce         : 0
    Cached         : 1984688
    Commit Limit   : 1988424
    Committed As   : 3358528
    High Total     : 0
    High Free      : 0
    Low Total      : 3976852
    Low Free       : 1209900
    Mapped         : 520528
    NFS Unstable   : 0
    Page Tables    : 17328
    Slab           : 0
    VMmalloc Chunk : 1069542588
    VMmalloc Total : 1069547512
```

```
  VMmalloc Used  : 2588
  Writeback      : 0
  HugePages Total: 0
  HugePages Free : 0
  HugePages Rsvd : 0
  HugePage Size  : 2048

Swap (kB)
  Total          : 0
  Used           : 0
  Free           : 0
  Cached         : 0

Buffers (kB)     : 439528

Load Average
  1-Min          : 1.13
  5-Min          : 1.18
  15-Min         : 0.92
```

show platform software process slot switch

プラットフォーム ソフトウェア プロセスのスイッチ情報を表示するには、特権 EXEC モードで **show platform software process slot switch** コマンドを使用します。

show platform software process slot switch {*switch-number*| **active**| **standby**} {**0**| **F0**| **R0**} **monitor**[**cycles***no-of-times*[**interval***delay*[**lines***number*]]]

構文の説明

switch-number	スイッチ番号。
active	アクティブ インスタンスを指定します。
standby	スタンバイ インスタンスを指定します。
0	共有ポートアダプタ（SPA）インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor（ESP）スロット 0 を指定します。
R0	ルート プロセッサ（RP）スロット 0 を指定します。
monitor	実行中のプロセスをモニタします。
cycles*no-of-tmes*	（任意）monitor コマンドを実行する回数を設定します。有効な値は、1 ～ 4294967295 です。デフォルトは 5 分です。

interval*delay*	（任意）それぞれの遅延を設定します。有効値は 0 ～ 300 です。デフォルトは 3 です。
lines*number*	（任意）表示される出力の行数を設定します。有効値は 0 ～ 512 です。デフォルトは 0 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
Cisco IOS XE Denali 16.1.1	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 platform software process slot switch コマンドと **show processes cpu platform monitor location** コマンドの出力に、Linux **top** コマンドの出力が表示されます。これらのコマンドの出力には、Linux **top** コマンドで表示される「空きメモリ」と「使用メモリ」が表示されます。これらのコマンドによって「空きメモリ」と「使用メモリ」に表示される値は、その他のプラットフォーム メモリ関連 CLI の出力で表示される値とは一致しません。

次に、**show platform software process slot switch active R0 monitor** コマンドの出力例を示します。

```
Switch# show platform software process slot switch active R0 monitor

top - 00:01:52 up 1 day, 11:20,  0 users,  load average: 0.50, 0.68, 0.83
Tasks: 311 total,   2 running, 309 sleeping,   0 stopped,   0 zombie
Cpu(s):  7.4%us,  3.3%sy,  0.0%ni, 89.2%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   3976844k total,  3955036k used,    21808k free,   419312k buffers
Swap:        0k total,        0k used,        0k free,  1946764k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 5693 root      20   0  3448 1368  912 R    7  0.0   0:00.07 top
17546 root      20   0 2044m 244m  79m S    7  6.3 186:49.08 fed main event
18662 root      20   0 1806m 678m 263m S    5 17.5 215:32.38 linux_iosd-imag
30276 root      20   0  171m  42m  33m S    5  1.1 125:06.77 repm
17835 root      20   0  935m  74m  63m S    4  1.9  82:28.31 sif_mgr
18534 root      20   0  182m 150m  10m S    2  3.9   8:12.08 smand
    1 root      20   0  8440 4740 2184 S    0  0.1   0:09.52 systemd
    2 root      20   0     0    0    0 S    0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S    0  0.0   0:02.86 ksoftirqd/0
    5 root       0 -20     0    0    0 S    0  0.0   0:00.00 kworker/0:0H
    7 root      RT   0     0    0    0 S    0  0.0   0:01.44 migration/0
    8 root      20   0     0    0    0 S    0  0.0   0:00.00 rcu_bh
    9 root      20   0     0    0    0 S    0  0.0   0:23.08 rcu_sched
   10 root      20   0     0    0    0 S    0  0.0   0:58.04 rcuc/0
   11 root      20   0     0    0    0 S    0  0.0  21:35.60 rcuc/1
   12 root      RT   0     0    0    0 S    0  0.0   0:01.33 migration/1
```

関連コマンド

コマンド	説明
show processes cpu platform monitor location	IOS XE プロセスの CPU 使用率に関する情報を表示します。

show platform software status control-processor

プラットフォーム ソフトウェアの制御プロセッサのステータスを表示するには、特権 EXEC モードで **show platform software status control-processor** コマンドを使用します。

show platform software status control-processor[**brief**]

構文の説明

brief	（任意）プラットフォームの制御プロセッサのステータスのサマリーを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

Cisco IOS XE Denali 16.3.1 より前は、コマンド出力に表示される「空きメモリ」は基盤となる Linux カーネルから得ていました。使用可能な一部のメモリ チャンクは空きメモリと見なされていなかったため、この値は正確ではありませんでした。

Cisco IOS XE Denali 16.3.1 では、空きメモリは正確に計算されて、コマンド出力の Free Memory フィールドに表示されます。

次に、**show platform memory software status control-processor** コマンドの出力例を示します。

```
Switch# show platform software status control-processor

2-RP0: online, statistics updated 7 seconds ago
Load Average: healthy
```

```
  1-Min: 1.00, status: healthy, under 5.00
  5-Min: 1.21, status: healthy, under 5.00
  15-Min: 0.90, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2766284 (70%), status: healthy
  Free: 1210568 (30%)
  Committed: 3358008 (84%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  4.40, System:  1.70, Nice:  0.00, Idle: 93.80
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  3.80, System:  1.20, Nice:  0.00, Idle: 94.90
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  7.00, System:  1.10, Nice:  0.00, Idle: 91.89
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  4.49, System:  0.69, Nice:  0.00, Idle: 94.80
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

3-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.24, status: healthy, under 5.00
  5-Min: 0.27, status: healthy, under 5.00
  15-Min: 0.32, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2706768 (68%), status: healthy
  Free: 1270084 (32%)
  Committed: 3299332 (83%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  4.50, System:  1.20, Nice:  0.00, Idle: 94.20
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  5.20, System:  0.50, Nice:  0.00, Idle: 94.29
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  3.60, System:  0.70, Nice:  0.00, Idle: 95.69
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  3.00, System:  0.60, Nice:  0.00, Idle: 96.39
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

4-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.21, status: healthy, under 5.00
  5-Min: 0.24, status: healthy, under 5.00
  15-Min: 0.24, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1452404 (37%), status: healthy
  Free: 2524448 (63%)
  Committed: 1675120 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  2.30, System:  0.40, Nice:  0.00, Idle: 97.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  4.19, System:  0.69, Nice:  0.00, Idle: 95.10
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  4.79, System:  0.79, Nice:  0.00, Idle: 94.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  2.10, System:  0.40, Nice:  0.00, Idle: 97.50
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

9-RP0: unknown, statistics updated 4 seconds ago
Load Average: healthy
  1-Min: 0.20, status: healthy, under 5.00
```

```
  5-Min: 0.35, status: healthy, under 5.00
  15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1451328 (36%), status: healthy
  Free: 2525524 (64%)
  Committed: 1675932 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.90, System:  0.50, Nice:  0.00, Idle: 97.60
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  4.39, System:  0.19, Nice:  0.00, Idle: 95.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  5.70, System:  1.00, Nice:  0.00, Idle: 93.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  1.30, System:  0.60, Nice:  0.00, Idle: 98.00
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
```

次に、**show platform memory software status control-processor brief** コマンドの出力例を示します。

```
Switch# show platform software status control-processor brief

Load Average
 Slot  Status  1-Min  5-Min 15-Min
2-RP0 Healthy   1.10   1.21   0.91
3-RP0 Healthy   0.23   0.27   0.31
4-RP0 Healthy   0.11   0.21   0.22
9-RP0 Healthy   0.10   0.30   0.34

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
2-RP0 Healthy  3976852  2766956 (70%)  1209896 (30%)   3358352 (84%)
3-RP0 Healthy  3976852  2706824 (68%)  1270028 (32%)   3299276 (83%)
4-RP0 Healthy  3976852  1451888 (37%)  2524964 (63%)   1675076 (42%)
9-RP0 Healthy  3976852  1451580 (37%)  2525272 (63%)   1675952 (42%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
2-RP0    0   4.10   2.00   0.00  93.80   0.00   0.10   0.00
         1   4.60   1.00   0.00  94.30   0.00   0.10   0.00
         2   6.50   1.10   0.00  92.40   0.00   0.00   0.00
         3   5.59   1.19   0.00  93.20   0.00   0.00   0.00
3-RP0    0   2.80   1.20   0.00  95.90   0.00   0.10   0.00
         1   4.49   1.29   0.00  94.20   0.00   0.00   0.00
         2   5.30   1.60   0.00  93.10   0.00   0.00   0.00
         3   5.80   1.20   0.00  93.00   0.00   0.00   0.00
4-RP0    0   1.30   0.80   0.00  97.89   0.00   0.00   0.00
         1   1.30   0.20   0.00  98.50   0.00   0.00   0.00
         2   5.60   0.80   0.00  93.59   0.00   0.00   0.00
         3   5.09   0.19   0.00  94.70   0.00   0.00   0.00
9-RP0    0   3.99   0.69   0.00  95.30   0.00   0.00   0.00
         1   2.60   0.70   0.00  96.70   0.00   0.00   0.00
         2   4.49   0.89   0.00  94.60   0.00   0.00   0.00
         3   2.60   0.20   0.00  97.20   0.00   0.00   0.00
```

show processes cpu platform monitor

IOS XE プロセスの CPU 使用率に関する情報を表示するには、特権 EXEC モードで **show processes cpu platform monitor** コマンドを使用します。

構文の説明

location	Field Replaceable Unit（FRU）の場所に関する情報を表示します。
show processes cpu platform monitor location switch	{*switch-number*|**active**|**standby**}{**0**|**F0**|**R0**}

switch	スイッチを指定します。
switch-number	スイッチ番号。
active	アクティブ インスタンスを指定します。
standby	スタンバイ インスタンスを指定します。
0	共有ポート アダプタ（SPA）インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor（ESP）スロット 0 を指定します。
R0	ルート プロセッサ（RP）スロット 0 を指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	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 platform software process slot switch コマンドと **show processes cpu platform monitor location** コマンドの出力に、Linux **top** コマンドの出力が表示されます。これらのコマンドの出力には、Linux **top** コマンドで表示される「空きメモリ」と「使用メモリ」が表示されます。これらのコマンドによって「空きメモリ」と「使用メモリ」に表示される値は、その他のプラットフォーム メモリ関連 CLI の出力で表示される値とは一致しません。

次に、**show processes cpu monitor location switch active R0** コマンドの出力例を示します。

```
Switch# show processes cpu platform monitor location switch active R0

top - 00:04:21 up 1 day, 11:22,  0 users,  load average: 0.42, 0.60, 0.78
Tasks: 312 total,   4 running, 308 sleeping,   0 stopped,   0 zombie
Cpu(s):  7.4%us,  3.3%sy,  0.0%ni, 89.2%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   3976844k total,  3956928k used,    19916k free,   419312k buffers
Swap:        0k total,        0k used,        0k free,  1947036k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 6294 root      20   0  3448 1368  912 R    9  0.0   0:00.07 top
17546 root      20   0 2044m 244m  79m S    7  6.3 187:02.07 fed main event
30276 root      20   0  171m  42m  33m S    7  1.1 125:15.54 repm
   16 root      20   0     0    0    0 S    5  0.0  22:07.92 rcuc/2
   21 root      20   0     0    0    0 R    5  0.0  22:13.24 rcuc/3
18662 root      20   0 1806m 678m 263m R    5 17.5 215:47.59 linux_iosd-imag
   11 root      20   0     0    0    0 S    4  0.0  21:37.41 rcuc/1
10333 root      20   0  6420 3916 1492 S    4  0.1   4:47.03 btrace_rotate.s
```

```
   10 root      20   0     0    0    0 S    2  0.0   0:58.13 rcuc/0
 6304 root      20   0   776   12    0 R    2  0.0   0:00.01 ls
17835 root      20   0  935m  74m  63m S    2  1.9  82:34.07 sif_mgr
    1 root      20   0  8440 4740 2184 S    0  0.1   0:09.52 systemd
    2 root      20   0     0    0    0 S    0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S    0  0.0   0:02.86 ksoftirqd/0
    5 root       0 -20     0    0    0 S    0  0.0   0:00.00 kworker/0:0H
    7 root      RT   0     0    0    0 S    0  0.0   0:01.44 migration/0
```

関連コマンド

コマンド	説明
show platform software process slot switch	プラットフォーム ソフトウェア プロセスのスイッチ情報を表示します。

show processes memory platform

Cisco IOS XE プロセスごとのメモリ使用率を表示するには、特権 EXEC モードで **show processes memory platform** コマンドを使用します。

show processes memory platform [**detailed**{**name***process-name*| **process-id***process-ID*} [**location**| **maps**[**location**] | **smaps**[**location**]] | **location**| **sorted**[**location**]] **switch**{*switch-number*| **active**| **standby**} {**0**| **F0**| **R0**}

構文の説明

detailed*process-name*	（任意）指定された Cisco IOS XE プロセスの詳細なメモリ情報を表示します。
name*process-name*	（任意）Cisco IOS XE プロセス名と一致します。
process-id*process-ID*	（任意）Cisco IOS XE プロセス ID と一致します。
location	（任意）FRU の場所に関する情報を表示します。
maps	（任意）プロセスのメモリ マップを表示します。
smaps	（任意）プロセスの smap を表示します。
sorted	（任意）Cisco IOS XE プロセスによって使用されている合計メモリに基づいてソートされた出力を表示します。

switch*switch-number*	デバイスに関する情報を表示します。
active	スイッチのアクティブインスタンスに関する情報を表示します。
standby	スイッチのスタンバイインスタンスに関する情報を表示します。
0	SPA プロセッサ間スロット 0 に関する情報を表示します。
F0	Embedded Service Processor（ESP）スロット 0 に関する情報を表示します。
R0	ルートプロセッサ（RP）スロット 0 に関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	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 XE Denali 16.3.1 より前は、コマンド出力に表示される「空きメモリ」は基盤となる Linux カーネルから得ていました。使用可能な一部のメモリ チャンクは空きメモリと見なされていなかったため、この値は正確ではありませんでした。

Cisco IOS XE Denali 16.3.1 では、空きメモリは正確に計算されて、コマンド出力の Free Memory フィールドに表示されます。

次に、**show processes memory platform** コマンドの出力例を示します。

```
Switch# show processes memory platform

System memory: 3976852K total, 2761580K used, 1215272K free,
Lowest: 1215272K
   Pid    Text      Data   Stack   Dynamic       RSS     Total              Name
-------------------------------------------------------------------------------
     1    1246      4400     132      1308      4400      8328           systemd
    96     233      2796     132       132      2796     12436   systemd-journal
   105     284      1796     132       176      1796      5208     systemd-udevd
   707      52      2660     132       172      2660     11688        in.telnetd
   744     968      3264     132      1700      3264      5800         brelay.sh
   835      52      2660     132       172      2660     11688        in.telnetd
   863     968      3264     132      1700      3264      5800         brelay.sh
```

```
   928     968      3996     132      2312      3996      6412      reflector.sh
   933     968      3976     132      2312      3976      6412       droputil.sh
   934     968      2140     132       528      2140      4628            oom.sh
   936     173       936     132       132       936      3068           xinetd
   945     968      1472     132       132      1472      4168       libvirtd.sh
   947     592     43164     132      3096     43164    154716             repm
   954      45       932     132       132       932      3132          rpcbind
   986     482      3476     132       132      3476    169288         libvirtd
   988      66       940     132       132       940      2724        rpc.statd
   993     968       928     132       132       928      4232   boothelper_evt.
  1017      21       640     132       132       640      2500      inotifywait
  1089     102      1200     132       132      1200      3328       rpc.mountd
  1328       9      2940     132       148      2940     13844            rotee
  1353      39       532     132       132       532      2336            sleep
!
!
!
```

次に、**show processes memory platform information** コマンドの出力例を示します。

```
Switch# show processes memory platform location switch active R0

System memory: 3976852K total, 2762844K used, 1214008K free,
Lowest: 1214008K
   Pid    Text      Data    Stack   Dynamic       RSS     Total               Name
--------------------------------------------------------------------------------
     1    1246      4400      132      1308      4400      8328            systemd
    96     233      2796      132       132      2796     12436    systemd-journal
   105     284      1796      132       176      1796      5208      systemd-udevd
   707      52      2660      132       172      2660     11688         in.telnetd
   744     968      3264      132      1700      3264      5800          brelay.sh
   835      52      2660      132       172      2660     11688         in.telnetd
   863     968      3264      132      1700      3264      5800          brelay.sh
   928     968      3996      132      2312      3996      6412       reflector.sh
   933     968      3976      132      2312      3976      6412        droputil.sh
!
!
!
```

次に、**show processes memory platform sorted** コマンドの出力例を示します。

```
Switch# show processes memory platform sorted

System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K
   Pid    Text      Data    Stack   Dynamic       RSS     Total               Name
--------------------------------------------------------------------------------
  9655    3787    264964      136     18004    264964   2675968                wcm
 17261     324    248588      132    103908    248588   2093076     fed main event
  7885  149848    684864      136        80    684864   1853548    linux_iosd-imag
 17891     398     75772      136      1888     75772    958240           sif_mgr
 17067    1087     77912      136      1796     77912    702184       platform_mgr
  4268     391    102084      136      5596    102084    482656          cli_agent
  4856     357     93388      132      3680     93388    340052                dbm
 29842    8722     64428      132      8056     64428    297068      fman_fp_image
  5960    9509     76088      136      3200     76088    287156           fman_rp
!
!
!
```

次に、**show processes memory platform sorted location switch active R0** コマンドの出力例を示します。

```
Switch# show processes memory platform sorted location switch active R0

System memory: 3976852K total, 2763584K used, 1213268K free,
Lowest: 1213268K
   Pid    Text      Data    Stack   Dynamic       RSS     Total               Name
--------------------------------------------------------------------------------
```

```
  9655    3787    264968     136     18004    264968   2675968              wcm
 17261     324    249020     132    103908    249020   2093076    fed main event
  7885  149848    684912     136        80    684912   1853548   linux_iosd-imag
 17891     398     75884     136      1888     75884    958240          sif_mgr
 17067    1087     77820     136      1796     77820    702184      platform_mgr
  4268     391    102084     136      5596    102084    482656         cli_agent
  4856     357     93388     132      3680     93388    340052              dbm
 29842    8722     64428     132      8056     64428    297068     fman_fp_image
  5960    9509     76088     136      3200     76088    287156           fman_rp
!
!
!
```

show power inline

指定された PoE ポート、指定されたスタック メンバ、またはスイッチ スタックのすべての PoE ポートの PoE ステータスを表示するには、EXEC モードで **show power inline** コマンドを使用します。

show power inline [**police**| **priority**] [*interface-id*| **module** *stack-member-number*] **[detail]**

構文の説明

police	（任意）リアルタイムの電力消費に関するパワー ポリシング情報を表示します。
priority	（任意）各ポートのパワーインライン ポート プライオリティを表示します。
interface-id	（任意）物理インターフェイスの ID です。
module*stack-member-number*	（任意）指定されたスタック メンバのポートだけを表示します。 指定できる範囲は 1 ～ 9 です。 このキーワードは、スタック対応スイッチでのみサポートされています。
detail	（任意）インターフェイスまたはモジュールの詳細な出力を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show power inline** コマンドの出力を示します。次の表に、出力フィールドについて説明します。

```
Device> show power inline
Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1             n/a        n/a         n/a
2             n/a        n/a         n/a
3          1440.0       15.4      1424.6
4           720.0        6.3       713.7
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi3/0/1   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/2   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/3   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/4   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/5   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/6   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/7   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/8   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/9   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/10  auto   off        0.0     n/a                 n/a   30.0
Gi3/0/11  auto   off        0.0     n/a                 n/a   30.0
Gi3/0/12  auto   off        0.0     n/a                 n/a   30.0
<output truncated>
```

次の例では、スイッチ ポートに対する **show power inline***interface-id* コマンドの出力を示します。

```
Device> show power inline gigabitethernet1/0/1
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/1   auto   off        0.0     n/a                 n/a   30.0
```

次の例では、スタック メンバ 3 での **show power inline module***switch-number* コマンドの出力を示します。次の表に、出力フィールドについて説明します。

```
Device> show power inline module 3
Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
3           865.0      864.0         1.0
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi3/0/1   auto   power-deny 4.0     n/a                 n/a   15.4
Gi3/0/2   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/3   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/4   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/5   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/6   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/7   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/8   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/9   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/10  auto   off        0.0     n/a                 n/a   15.4
```

```
<output truncated>
```

表 *17* : ***show power inline*** のフィールドの説明

フィールド	説明
Available	PoE スイッチ上の設定電力[3]の合計で、ワット数（W）です。
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計（ワット数）です。（Available - Used = Remaining）
Admin	管理モード：auto、off、static
Oper	動作モード： • on：受電デバイスが検出され、電力が適用されています。 • off：PoE が適用されていません。 • faulty：装置検出または受電デバイスが障害の状態です。 • power-deny：受電デバイスが検出されていますが、PoE が使用できない状態か、最大ワット数が検出された受電デバイスの最大数を超えています。
電源	受電デバイスに割り当てられている最大電力の合計で、ワット数です。この値は、**show power inline police** コマンドの出力の *Cutoff Power* フィールドの値と同じです。
デバイス	検出された装置のタイプ：n/a、unknown、Cisco 受電装置、IEEE 受電装置、または CDP からの名前。
クラス	IEEE 分類：n/a または 0 ～ 4 の値。
Max	受電デバイスに割り当てられている最大電力の合計で、ワット数です。

フィールド	説明
AdminPowerMax	スイッチがリアルタイム電力消費をポリシングする場合に、受電デバイスに割り当てられる電力の最大量です（ワット単位）。この値は、*Max* フィールドの値と同じです。
AdminConsumption	スイッチがリアルタイム電力消費をポリシングする場合に、受電デバイスに割り当てられる電力の消費量です（ワット単位）。ポリシングがディセーブルである場合、この値は *AdminPowerMax* フィールドの値と同じです。

[3] 設定電力とは、手動で指定する電力、またはCDP電力ネゴシエーションまたはIEEE分類を使用してスイッチが指定する電力です（電力検知機能によってモニタされるリアルタイムの電力とは異なります）。

次の例では、スタッキング対応スイッチに対する **show power inline police** コマンドの出力を示します。

```
Device> show power inline police
Module   Available     Used      Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1            370.0        0.0       370.0
3            865.0      864.0         1.0
          Admin  Oper         Admin      Oper       Cutoff Oper
Interface State  State        Police     Police     Power  Power
--------- ------ ------------ ---------- ---------- ------ ------
Gi1/0/1   auto   off          none       n/a        n/a    0.0
Gi1/0/2   auto   off          log        n/a        5.4    0.0
Gi1/0/3   auto   off          errdisable n/a        5.4    0.0
Gi1/0/4   off    off          none       n/a        n/a    0.0
Gi1/0/5   off    off          log        n/a        5.4    0.0
Gi1/0/6   off    off          errdisable n/a        5.4    0.0
Gi1/0/7   auto   off          none       n/a        n/a    0.0
Gi1/0/8   auto   off          log        n/a        5.4    0.0
Gi1/0/9   auto   on           none       n/a        n/a    5.1
Gi1/0/10  auto   on           log        ok         5.4    4.2
Gi1/0/11  auto   on           log        log        5.4    5.9
Gi1/0/12  auto   on           errdisable ok         5.4    4.2
Gi1/0/13  auto   errdisable   errdisable n/a        5.4    0.0
<output truncated>
```

上の例では、次のようになっています。

- Gi1/0/1 ポートはシャットダウンしていて、ポリシングは設定されていません。
- Gi1/0/2 ポートはシャットダウンしていますが、ポリシングはイネーブルであり、ポリシングアクションとして syslog メッセージを生成するよう設定されています。
- Gi1/0/3 ポートはシャットダウンしていますが、ポリシングはイネーブルであり、ポリシングアクションとしてポートをシャットダウンするよう設定されています。
- Gi1/0/4 ポートでは、デバイス検出がディセーブルであり、ポートに電力が供給されておらず、ポリシングがディセーブルです。

- Gi1/0/5 ポートでは、デバイス検出がディセーブルであり、ポートに電力が供給されていませんが、ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されています。
- Gi1/0/6 ポートでは、デバイス検出がディセーブルであり、ポートに電力が供給されていませんが、ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。
- Gi1/0/7 ポートはアップしていて、ポリシングはディセーブルですが、接続されている装置に対してスイッチから電力が供給されていません。
- Gi1/0/8 ポートはアップしていて、ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されていますが、受電デバイスに対してスイッチから電力が供給されていません。
- Gi1/0/9 ポートはアップしていて、受電デバイスが接続されており、ポリシングはディセーブルです。
- Gi1/0/10 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されています。リアルタイム電力消費がカットオフ値より少ないため、ポリシング アクションは作動しません。
- Gi1/0/11 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されています。
- Gi1/0/12 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。リアルタイム電力消費がカットオフ値より少ないため、ポリシング アクションは作動しません。
- Gi1/0/13 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。

次の例では、スタンドアロン スイッチに対する **show power inline police***interface-id* コマンドの出力を示します。次の表に、出力フィールドについて説明します。

```
Device> show power inline police gigabitethernet1/0/1
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi1/0/1   auto   off        none       n/a        n/a    0.0
```

表 *18*：*show power inline police* のフィールドの説明

フィールド	説明
Available	スイッチ上の設定電力[4]の合計で、ワット数（W）です。

フィールド	説明
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計（ワット数）です。（Available - Used = Remaining）
Admin State	管理モード：auto、off、static
Oper State	動作モード： • errdisable：ポリシングはイネーブルです。 • faulty：受電デバイスでの装置検出が障害の状態です。 • off：PoE が適用されていません。 • on：受電デバイスが検出され、電力が適用されています。 • power-deny：受電デバイスが検出されていますが、PoE が使用できない状態か、リアルタイム電力消費が最大電力割り当てを超えています。 （注） 動作モードは、指定した PoE ポート、指定したスタック メンバ、またはスイッチのすべての PoE ポートの現在の PoE ステートです。
Admin Police	リアルタイム電力消費ポリシング機能のステータス： • errdisable：ポリシングがイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチはポートをシャットダウンします。 • log：ポリシングはイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチが Syslog メッセージを生成します。 • none：ポリシングはディセーブルです。

フィールド	説明
Oper Police	ポリシング ステータス： • errdisable：リアルタイム電力消費が最大電力割り当てを超えています。スイッチがPoE ポートをシャットダウンします。 • log：リアルタイム電力消費が最大電力割り当てを超えています。スイッチがSyslogメッセージを生成します。 • n/a：装置検出がディセーブルで、電力がPoEポートに適用されていないか、ポリシング アクションが設定されていません。 • ok：リアルタイム電力消費が最大電力割り当てより少ない状態です。
Cutoff Power	ポートに割り当てられている最大電力です。リアルタイム電力消費がこの値を上回ると、スイッチは設定されたポリシングアクションを実行します。
Oper Power	受電デバイスのリアルタイム電力消費です。

[4] 設定電力とは、手動で指定する電力、またはCDP電力ネゴシエーションまたはIEEE分類を使用してスイッチが指定する電力（電力検知機能によってモニタされるリアルタイムの電力とは異なります）です。

関連トピック

logging event power-inline-status, （163 ページ）

power inline, （173 ページ）

show stack-power

電源スタックのStackPower スタックまたはスイッチに関する情報を表示するには、EXEC モードで **show stack-power** コマンドを使用します。

{**show stack-power** [**budgeting**| **detail**| **load-shedding**| **neighbors**] [**order** *power-stack-name*]| [**stack-name** [*stack-id*]| **switch** [*switch-id*]]}

構文の説明

budgeting	（任意）スタック電源のバジェット テーブルを表示します。
detail	（任意）スタック電源のスタックの詳細を表示します。

load-shedding	（任意）スタック電源の負荷制限テーブルを表示します。
ネイバー	（任意）スタック電源のネイバー テーブルを表示します。
order*power-stack-name*	（任意）電源スタックの負荷制限優先順位を表示します。 （注） このキーワードは、**load-shedding** キーワードの後にのみ使用できます。
stack-name	（任意）すべての電源スタックまたは指定された電源スタックのバジェット テーブル、詳細、またはネイバーを表示します。 （注） このキーワードは、**load-shedding** キーワードの後には使用できません。
stack-id	（任意）電源スタックの電源スタック ID。スタック ID は、31 文字以下である必要があります。
switch	（任意）すべてのスイッチ、または指定されたスイッチのバジェット テーブル、詳細、負荷制限、またはネイバーを表示します。
switch-id	（任意）スイッチのスイッチ ID。スイッチ番号は 1～9 です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	すべてのオプションのサポートは、このコマンドに対して有効になっています。
Cisco IOS XE Denali 16.1.1	このコマンドが再度導入されました。

使用上のガイドライン

このコマンドは、IP Base または IP Services イメージが実行されているスイッチ スタックでのみ使用できます。

負荷制限のためにスイッチがシャットダウンされた場合、**show stack-power** コマンドの出力には、シャットダウンされたネイバー スイッチの MAC アドレスが含まれています。コマンド出力は、スイッチに供給するために十分な電力がない場合でも、スタック電力トポロジを示します。

次の例では、**show stack-power** コマンドの出力を示します。

```
Device# show stack-power
Power Stack           Stack   Stack    Total   Rsvd    Alloc   Unused  Num  Num
Name                  Mode    Topolgy  Pwr(W)  Pwr(W)  Pwr(W)  Pwr(W)  SW   PS
--------------------  ------  -------  ------  ------  ------  ------  ---  ---
Powerstack-1          SP-PS   Stndaln  350     150     200     0       1    1
```

次の例では、**show stack-power budgeting** コマンドの出力を示します。

```
Device# show stack-power budgeting
Power Stack           Stack   Stack    Total   Rsvd    Alloc   Unused  Num  Num
Name                  Mode    Topolgy  Pwr(W)  Pwr(W)  Pwr(W)  Pwr(W)  SW   PS
--------------------  ------  -------  ------  ------  ------  ------  ---  ---
Powerstack-1          SP-PS   Stndaln  350     150     200     0       1    1

    Power Stack           PS-A   PS-B   Power     Alloc     Avail   Consumd Pwr
SW  Name                  (W)    (W)    Budgt(W)  Power(W)  Pwr(W)  Sys/PoE(W)
--  --------------------  -----  -----  --------  --------  ------  -----------
1   Powerstack-1          350    0      200       200       0       60   /0
--  --------------------  -----  -----  --------  --------  ------  -----------
Totals:                                          200       0       60   /0
```

show system mtu

グローバル最大伝送ユニット（MTU）、またはスイッチに設定されている最大パケットサイズを表示するには、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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

MTU 値および MTU 値に影響を与えるスタック設定の詳細については、**system mtu** コマンドを参照してください。

次の例では、**show system mtu** コマンドの出力を示します。

```
Device# show system mtu
Global Ethernet MTU is 1500 bytes.
```

関連トピック

system mtu, （259 ページ）

show tech-support

システム情報を表示する **show** コマンドを自動的に実行するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support[**cef**| **cft**| **eigrp**| **evc**| **fnf**| **ipc**| **ipmulticast**| **ipsec**| **mfib**| **nat**| **nbar**| **onep**| **ospf**| **page**| **password**| **rsvp**| **subscriber**| **vrrp**| **wccp**| **wireless**]

構文の説明

cef	（任意）CEF 関連情報を表示します。
cft	（任意）CFT 関連情報を表示します。
eigrp	（任意）EIGRP 関連情報を表示します。
evc	（任意）EVC 関連情報を表示します。
fnf	（任意）Flexible NetFlow 関連情報を表示します。
ipc	（任意）IPC 関連情報を表示します。
ipmulticast	（任意）IP 関連情報を表示します。
ipsec	（任意）IPSEC 関連情報を表示します。
mfib	（任意）MFIB 関連情報を表示します。
nat	（任意）NAT 関連情報を表示します。
nbar	（任意）NBAR 関連情報を表示します。
onep	（任意）ONEP 関連情報を表示します。

ospf	（任意）OSPF 関連情報を表示します。
page	（任意）コマンド出力を 1 ページずつ表示します。Return キーを押して、出力の次の行を表示するか、スペースバーを使用して、次の情報ページを表示します。使用しない場合、出力がスクロールします（つまり、改ページで停止しません）。 コマンド出力を停止するには、**Ctrl+C** キーを押します。
password	（任意）パスワードおよびその他のセキュリティ情報を出力に残します。使用しない場合、出力中のパスワードおよびそのほかのセキュリティ関連情報は、ラベル「<removed>」と置き換えられます。
rsvp	（任意）IP RSVP 関連情報を表示します。
subscriber	（任意）サブスクライバ関連情報を表示します。
vrrp	（任意）VRRP 関連情報を表示します。
wccp	（任意）WCCP 関連情報を表示します。
wireless	（任意）ワイヤレス関連情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドは、出力修飾子の次のコマンドの出力を表示できるよう強化されました。 • **show power inline** • **show platform software ilpower details** • **show power inline police** • **show stack-power budgeting**
Cisco IOS XE Denali 16.1.1	このコマンドが再度導入されました。

使用上のガイドライン

show tech-support コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします（たとえば、**show tech-support** > filename）。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center（TAC）の担当者に送信することも容易になります。

リダイレクトには、次のいずれかの方法を使用できます。

- > *filename*：出力をファイルにリダイレクトします。
- >> filename：出力をファイルにアペンド モードでリダイレクトします。

show wireless interface summary

ワイヤレス インターフェイスのステータスおよび設定を表示するには、**show wireless interface summary** 特権 EXEC コマンドを使用します。

show wireless interface summary

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

次に、ワイヤレス インターフェイスの要約を表示する例を示します。

```
Device# show wireless interface summary
```

speed

10/100/1000/2500/5000 Mbps ポートの速度を指定するには、インターフェイス コンフィギュレーション モードで **speed** 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。

speed {**10**| **100**| **1000**| **2500**| **5000**| **auto** [**10**| **100**| **1000**| **2500**| **5000**]| **nonegotiate**}

no speed

構文の説明

10	ポートが 10 Mb/s で稼働することを指定します。
100	ポートが 100 Mb/s で稼働することを指定します。
1000	ポートが 1000 Mb/s で稼働することを指定します。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。
2500	ポートが 2500 Mb/s で稼働することを指定します。このオプションは、mGig 対応のイーサネット ポートでのみ有効であり表示されます。
5000	ポートが 5000 Mb/s で稼働することを指定します。このオプションは、mGig 対応のイーサネット ポートでのみ有効であり表示されます。
auto	リンクのもう一方の終端のポートを基準にして自動的にポートの速度を検出します。**10**、**100**、**1000**、**1000**、**2500**、**5000** のキーワードと **auto** キーワードを一緒に使用する場合、ポートは指定された速度でのみ自動ネゴシエーションを行います。
nonegotiate	自動ネゴシエーションをディセーブルにし、ポートは 1000 Mb/s で稼働します。

コマンド デフォルト

デフォルトは **auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが変更されました。次のキーワードが追加されました。2500 と 5000。これらのキーワードは、mGig 対応デバイスでのみ表示されます。

使用上のガイドライン

10 ギガビット イーサネット ポートでは速度を設定できません。

1000BASE-T Small Form-Factor Pluggable（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は、ネゴシエートしないように（**nonegotiate**）速度を設定できます。

新しいキーワード（2500 と 5000）は、mGig 対応デバイスでのみ表示されます。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にある装置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では自動ネゴシエーションをサポートし、もう一方の終端で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。

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

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。

```
Device(config)# interface gigabitethernet1/0/1
Device(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。

```
Device(config)# interface gigabitethernet1/0/1
Device(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。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10 100
```

関連トピック

duplex, （148 ページ）

show interfaces, （205 ページ）

stack-power

設定内容 電源スタックまたは電源スタックのスイッチにStackPower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 **stack power** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

stack-power {**stack** *power-stack-name*| **switch** *stack-member-number*}

no stack-power {**stack** *power-stack-name*| **switch** *stack-member-number*}

構文の説明

stack*power-stack-name*	電源スタックの名前を指定します。名前は最大で31文字にできます。これらのキーワードの後に改行を入力すると、電源スタック コンフィギュレーション モードが開始されます。
switch*stack-member-number*	スタックのスイッチ番号（1 ～ 4）を指定して、スイッチのスイッチスタック電源コンフィギュレーション モードを開始します。

コマンド デフォルト

デフォルトはありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

stack-power stack *power stack name* コマンドを入力すると、電源スタック コンフィギュレーション モードが開始され、次の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。
- **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。
- **mode**：電源スタックの電源モードを設定します。**mode** コマンドを参照してください。
- **no**：コマンドを無効にするか、デフォルト設定に戻します。

StackPower に関係のないスイッチ番号を指定して **stack-power switch** *switch-number* 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。

StackPower に関係するスイッチ番号を指定して **stack-power switch** *switch-number* コマンドを入力すると、スイッチスタック電源コンフィギュレーションモードが開始され、次の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。
- **exit**：スイッチ スタック電源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。
- **power-priority**：スイッチおよびスイッチ ポートの電源プライオリティを設定します。**power-priority** コマンドを参照してください。
- **stack-id***name*：スイッチが属する電源スタックの名前を入力します。電源スタック ID を入力しない場合、スイッチはスタック パラメータを継承しません。名前は最大で 31 文字にできます。
- **standalone**：スイッチをスタンドアロン電源モードで動作させます。このモードに設定すると、両方の電源ポートがシャットダウンします。

次の例では、電源スタックに接続されたスイッチ 2 が電源プールから削除され、両方の電源ポートがシャットダウンされます。

```
Device(config)# stack-power switch 2
Device(config-switch-stackpower)# standalone
Device(config-switch-stackpower)# exit
```

関連トピック

mode（電源スタックの設定），（165 ページ）

power-priority，（171 ページ）

show stack-power

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、インターフェイス コンフィギュレーション モードで **switchport block** コマンドを使用します。不明のマルチキャストまたはユニキャスト パケットの転送を許可するには、このコマンドの **no** 形式を使用します。

switchport block {**multicast**| **unicast**}

no switchport block {**multicast**| **unicast**}

構文の説明

multicast	不明のマルチキャスト トラフィックがブロックされるように指定します。 （注） 純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
unicast	不明のユニキャスト トラフィックがブロックされるように指定します。

コマンド デフォルト

不明なマルチキャストおよびユニキャスト トラフィックはブロックされていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

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。

```
Device(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。

関連トピック

show interfaces switchport, （212 ページ）

system mtu

ギガビット イーサネットおよび 10 ギガビット イーサネット ポートのスイッチド パケットのグローバル最大パケット サイズまたは MTU 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 **system mtu** 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*

no system mtu

構文の説明

bytes	グローバル MTU のサイズ（バイト単位）。指定できる範囲は、1500 ～ 9198 バイトです。デフォルトは 1500 バイトです。

コマンド 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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

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

スイッチはインターフェイス単位では MTU をサポートしていません。

特定のインターフェイス タイプで許容範囲外の値を入力した場合、その値は受け入れられません。

次に、グローバル システム MTU サイズを 6000 バイトに設定する例を示します。

```
Device(config)# system mtu 6000
Global Ethernet MTU is set to 6000 bytes.
Note: this is the Ethernet payload size, not the total
Ethernet frame size, which includes the Ethernet
header/trailer and possibly other tags, such as ISL or
802.1q tags.
```

関連トピック

show system mtu, （250 ページ）

test mcu read-register

Power over Ethernet（PoE）コントローラのデバッグを有効にするには、特権 EXEC モードで **test mcu read-register** コマンドを使用します。

test mcu read-register {**det-cls-offset**| **manufacture-id**| **port-mode**}

構文の説明

det-cls-offset	読み取り検出分類登録の概要を表示します。
manufacture-id	PoE コントローラの製造 ID を表示します。
port-mode	ポート モードの詳細を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE Denali 16.3.2	このコマンドが導入されました。

次に、**test mcu read-register det-cls-offset** コマンドの出力例を示します。

```
Device# test mcu read-register det-cls-offset 1
 DETECTION ENABLE BIT SUMMARY

Controller    port1          port2          port3          port4       register
                                                                      (hexadecimal)
----------   -------        -------        -------        -------     ------------
1               1              0              1              0           5

2               1              0              1              0           5

3               1              0              1              0           5
```

```
4               1               0               1               0               5
5               1               0               1               0               5
6               1               0               1               0               5
7               1               0               1               0               5
8               1               0               1               0               5
9               1               0               1               0               5
10              1               0               1               0               5
11              0               0               1               0               4
12              1               0               0               0               1
 CLASSIFICATION ENABLE BIT SUMMARY
Controller    port1          port2          port3          port4       register
                                                                      (hexadecimal)
----------   -------        -------        -------        -------    ------------
1               1               0               1               0               5
2               1               0               1               0               5
3               1               0               1               0               5
4               1               0               1               0               5
5               1               0               1               0               5
6               1               0               1               0               5
7               1               0               1               0               5
8               1               0               1               0               5
9               1               0               1               0               5
10              1               0               1               0               5
11              0               0               1               0               4
12              1               0               0               0               1
```

次に、**test mcu read-register manufacture-id** コマンドの出力例を示します。

```
MANUFACTURE ID : DEVICE_BCM_PALPATINE reg_val = 0x1B
```

次に、**test mcu read-register port-mode** コマンドの出力例を示します。

```
 PORT MODE SUMMERY
Controller    port1          port2          port3          port4       register
                                                                      (hexadecimal)
----------   -------        -------        -------        -------    ------------
1              01              00              01              00              22
2              01              00              01              00              22
3              01              00              01              00              22
4              01              00              01              00              22
5              01              00              01              00              22
6              01              00              01              00              22
7              01              00              01              00              22
8              01              00              01              00              22
```

9	01	00	01	00	22
10	01	00	01	00	22
11	00	00	01	00	20
12	01	00	00	00	2

voice-signalingvlan（ネットワークポリシーコンフィギュレーション）

音声シグナリング アプリケーション タイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice-signaling vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

voice-signaling vlan {*vlan-id* [**cos** *cos-value*| **dscp** *dscp-value*]| **dot1p** [**cos** *l2-priority*| **dscp** *dscp*]| **none**| **untagged**}

構文の説明

vlan-id	（任意）音声トラフィック用の VLAN。指定できる範囲は 1 ～ 4094 です。
cos *cos-value*	（任意）設定された VLAN に対するレイヤ 2 プライオリティ Class of Service（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。
dscp *dscp-value*	（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。デフォルト値は 46 です。
dot1p	（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。
none	（任意）音声 VLAN に関して IP Phone に指示しません。電話は電話のキーパッドから入力された設定を使用します。
untagged	（任意）タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

コマンド デフォルト

音声シグナリング アプリケーション タイプの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。

デフォルトの CoS 値は、5 です。

デフォルトの DSCP 値は、46 です。

デフォルトのタギング モードは、untagged です。

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 モードを開始するには、**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。

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。

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。

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。

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。

次の例では、プライオリティ 2 の CoS を持つ VLAN 200 用の音声シグナリングを設定する方法を示します。

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice-signaling vlan 200 cos 2
```

次の例では、DSCP 値 45 を持つ VLAN 400 用の音声シグナリングを設定する方法を示します。

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice-signaling vlan 400 dscp 45
```

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 用の音声シグナリングを設定する方法を示します。

```
Device(config-network-policy)# voice-signaling vlan dot1p cos 4
```

voice vlan（ネットワークポリシー コンフィギュレーション）

音声アプリケーション タイプのネットワークポリシープロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

voice vlan {*vlan-id* [**cos** *cos-value*| **dscp** *dscp-value*]| **dot1p** [**cos** *l2-priority*| **dscp** *dscp*]| **none**| **untagged**}

構文の説明

vlan-id	（任意）音声トラフィック用の VLAN。指定できる範囲は 1 ～ 4094 です。
cos *cos-value*	（任意）設定された VLAN に対するレイヤ 2 プライオリティ Class of Service（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。
dscp *dscp-value*	（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。デフォルト値は 46 です。
dot1p	（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。
none	（任意）音声 VLAN に関して IP Phone に指示しません。電話は電話のキーパッドから入力された設定を使用します。
untagged	（任意）タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

コマンド デフォルト

音声アプリケーション タイプの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。

デフォルトの CoS 値は、5 です。

デフォルトの DSCP 値は、46 です。

デフォルトのタギング モードは、untagged です。

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 モードを開始するには、**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。

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。

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、音声用のプロファイルを作成することができます。

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。

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。

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。

```
Device(config)# network-policy profile 1
Device(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。

```
Device(config)# network-policy profile 1
Device(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。

```
Device(config-network-policy)# voice vlan dot1p cos 4
```

wireless ap-manager interface

ワイヤレス AP マネージャ インターフェイスを設定するには、**wireless ap-manager interface** コマンドを使用します。

wireless ap-managerinterface {**TenGigabitEthernet** *interface-number*| **Vlan** *interface-number*}

構文の説明

TenGigabitEthernet*interface-name*	10 ギガビット イーサネット インターフェイスを設定します。値の範囲は 0 ～ 9 です。
Vlan*interface-name*	VLAN を設定します。値の範囲は 1 ～ 4095 です。

コマンド デフォルト

なしーバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例は、ワイヤレス AP-manager を設定する方法を示しています。

```
Device# wireless ap-manager interface vlan
<1-4095>  Vlan interface number
```

次の例は、ワイヤレス AP-manager を設定する方法を示しています。

```
Device# #wireless ap-manager interface vlan 10
```

wireless exclusionlist

除外リスト エントリを管理するには、**wireless exclusionlist** グローバル コンフィギュレーション コマンドを使用します。除外リスト 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。

wireless exclusionlist *mac-addr* **description** *description*

no wireless exclusionlist *mac-addr*

構文の説明

mac-addr	ローカル除外リスト エントリの MAC アドレス。
description*description*	除外リスト エントリの説明を指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、MAC アドレス xxx.xxx.xxx のローカル除外リスト エントリを作成する例を示します。

```
Device# wireless exclusionlist xxx.xxx.xxx
```

次に、MAC アドレス xxx.xxx.xxx のローカル除外リスト エントリの説明を作成する例を示します。

```
Device# wireless exclusionlist xxx.xxx.xxx description sample
```

wireless linktest

リンク テスト フレーム サイズおよび送信するフレーム数を設定するには、**wireless linktest** コマンドを使用します。

wireless linktest {**frame-size** *size*| **number-of-frames** *value*}

構文の説明

frame-size*size*	各パケットのリンク テスト フレームのサイズを指定します。値の範囲は 1 ～ 1400 です。
number-of-frames*value*	リンク テストに送信するフレーム数を指定します。値の範囲は 1 ～ 100 です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、各フレーム リンクのテスト フレームのサイズを 10 に設定する例を示します。

```
Device# wireless linktest frame-size 10
```

wireless management interface

インターフェイスのワイヤレス管理パラメータを設定するには、**wireless management interface** グローバルコンフィギュレーションコマンドを使用します。インターフェイスのワイヤレス管理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。

wireless management interface *interface-name* {**TenGigabitEthernet** *interface-name*| **Vlan** *interface-name*}

no wireless management interface

構文の説明

interface-name	インターフェイス番号
TenGigabitEthernet *interface-name*	10 ギガビット イーサネット インターフェイス番号。値の範囲は 0 ～ 9 です。
Vlan *interface-name*	VLAN インターフェイス番号。値の範囲は 1 ～ 4095 です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ワイヤレス インターフェイスに VLAN 10 を設定する例を示します。

```
Device# wireless management interface Vlan 10
```

wireless peer-blocking forward-upstream

アップストリーム転送のピアツーピア ブロッキングを設定するには、**wireless peer-blocking forward-upstream** コマンドを使用します。ピアツーピア ブロッキングを削除するには、このコマンドの **no** 形式を使用します。

wireless peer-blocking forward-upstream *interface*{**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

no wireless peer-blocking forward-upstream {**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

構文の説明

GigabitEthernet *interface*	ギガビット イーサネット インターフェイス番号。値の範囲は 0 ～ 9 です。
TenGigabitEthernet *interface*	10 ギガビット イーサネット インターフェイス番号。値の範囲は 0 ～ 9 です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、インターフェイスの 10 ギガビット イーサネット インターフェイスについてピアツーピア ブロッキングを設定する例を示します。

```
Device(config)# wireless peer-blocking forward-upstream TenGigabitEthernet 1/1/4
```

第 V 部

IP

- IP コマンド，273 ページ

第 6 章

IP コマンド

- clear ip nhrp, 274 ページ
- debug nhrp, 276 ページ
- fhrp delay, 278 ページ
- fhrp version vrrp v3, 279 ページ
- glbp authentication, 280 ページ
- glbp forwarder preempt, 281 ページ
- glbp ip, 282 ページ
- glbp load-balancing, 284 ページ
- glbp name, 285 ページ
- glbp preempt, 287 ページ
- glbp priority, 288 ページ
- glbp timers, 290 ページ
- glbp weighting, 292 ページ
- glbp weighting track, 294 ページ
- ip address dhcp, 296 ページ
- ip address pool (DHCP), 300 ページ
- ip address, 301 ページ
- ip nhrp map, 304 ページ
- ip nhrp map multicast, 306 ページ
- ip nhrp network-id, 308 ページ
- ip nhrp nhs, 309 ページ

- key chain, 312 ページ
- key-string（認証）, 313 ページ
- key, 314 ページ
- show glbp, 316 ページ
- show ip nhrp nhs, 320 ページ
- show key chain, 323 ページ
- show track, 324 ページ
- track, 326 ページ
- vrrp, 328 ページ
- vrrp description, 329 ページ
- vrrp preempt, 330 ページ
- vrrp priority, 331 ページ
- vrrp timers advertise, 333 ページ
- vrrs leader, 334 ページ

clear ip nhrp

Next Hop Resolution Protocol（NHRP）キャッシュ内のすべてのダイナミック エントリをクリアするには、ユーザ EXEC モードまたは特権 EXEC モードで **clear ip nhrp** コマンドを使用します。

clear ip nhrp[**vrf**{*vrf-name*| **global**}] [*dest-ip-address* [*dest-mask*] | **tunnel***number*| **counters**[**interfacetunnel***number*]| **stats**[**tunnel***number*[**vrf**{*vrf-name*| **global**}]]]

構文の説明

vrf	（任意）指定された Virtual Routing and Forwarding（VRF）インスタンスの NHRP キャッシュからエントリを削除します。
vrf-name	（任意）コマンドが適用された VRF アドレス ファミリの名前。
global	（任意）グローバル VRF インスタンスを指定します。
dest-ip-address	（任意）宛先 IP アドレス。この引数を指定すると、指定された宛先 IP アドレスの NHRP マッピング エントリがクリアされます。

dest-mask	（任意）宛先ネットワーク マスク。
counters	（任意）NHRP カウンタをクリアします。
interface	（任意）すべてのインターフェイスの NHRP マッピング エントリをクリアします。
tunnel*number*	（任意）NHRP キャッシュから指定されたインターフェイスを削除します。
stats	（任意）すべてのインターフェイスの IPv4 統計情報をすべてクリアします。

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
Cisco IOS XE Denali 16.3.1	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 nhrp コマンドでは、スタティックに設定された IP と NBMA のいずれのアドレス マッピングも NHRP キャッシュからクリアしません。

次に、インターフェイスの NHRP キャッシュ内のダイナミック エントリすべてをクリアする例を示します。

```
Switch# clear ip nhrp
```

関連コマンド

コマンド	説明
show ip nhrp	NHRP マッピング情報を表示します。

debug nhrp

Next Hop Resolution Protocol（NHRP）のデバッグを有効にするには、特権 EXEC モードで **debug nhrp** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug nhrp [**attribute**| **cache**| **condition**{**interface tunnel** *number*| **peer**{**nbma**{*ipv4-nbma-address*| *nbma-name*| *ipv6-nbma-address*} } | **umatched**| **vrf** *vrf-name*}| **detail**| **error**| **extension**| **group**| **packet**| **rate**]

no debug nhrp [**attribute**| **cache**| **condition**{**interface tunnel** *number*| **peer**{**nbma**{*ipv4-nbma-address*| *nbma-name*| *ipv6-nbma-address*} } **unmatched**| **vrf** *vrf-name*}| **detail**| **error**| **extension**| **group**| **packet**| **rate**]

構文の説明

attribute	（任意）NHRP 属性デバッグ操作を有効にします。
cache	（任意）NHRP キャッシュデバッグ操作を有効にします。
condition	（任意）NHRP 条件デバッグ操作を有効にします。
interface tunnel*number*	（任意）トンネルインターフェイスのデバッグ操作を有効にします。
nbma	（任意）ノンブロードキャスト マルチプル アクセス（NBMA）ネットワークのデバッグ操作を有効にします。
ipv4-nbma-address	（任意）NBMA ネットワークの IPv4 アドレスに基づくデバッグ操作を有効にします。
nbma-name	（任意）NBMA ネットワーク名。
IPv6-address	（任意）NBMA ネットワークの IPv6 アドレスに基づくデバッグ操作を有効にします。 （注） *IPv6-address* 引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。
vrf*vrf-name*	（任意）Virtual Routing and Forwarding インスタンスのデバッグ操作を有効にします。

detail	（任意）NHRP デバッグの詳細なログを表示します。
error	（任意）NHRP エラーデバッグ操作を有効にします。
extension	（任意）NHRP 拡張処理デバッグ操作を有効にします。
group	（任意）NHRP グループデバッグ操作を有効にします。
packet	（任意）NHRP アクティビティデバッグを有効にします。
rate	（任意）NHRP レート制限を有効にします。
routing	（任意）NHRP ルーティングデバッグ操作を有効にします。

コマンド デフォルト

NHRP デバッグは有効になっていません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

（注） Cisco IOS XE Denali 16.3.1 では、このコマンドは IPv4 だけをサポートしています。*IPv6-nbma-address* 引数は、スイッチでは使用可能ですが、設定しても機能しません。

NHRP 属性ログを表示するには、**debug nhrp detail** コマンドを使用します。

Virtual-Access*number* キーワード/引数ペアは、デバイスで仮想アクセス インターフェイスが使用可能な場合にのみ表示されます。

次に、**debugnhrp** コマンドの出力例と、IPv4 に関する NHRP デバッグ出力を表示する例を示します。

```
Switch# debug nhrp

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST 10.1.1.99
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.  Tunnel IP addr 10.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486:       src: 10.1.1.11, dst: 10.1.1.99
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
Aug  9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

関連コマンド

コマンド	説明
showipnhrp	NHRP マッピング情報を表示します。

fhrp delay

First Hop Redundancy Protocol（FHRP）クライアントの初期化の遅延時間を指定するには、インターフェイス コンフィギュレーション モードで **fhrp delay** コマンドを使用します。指定した時間を削除するには、このコマンドの **no** 形式を使用します。

fhrp delay {[**minimum**] [**reload**] *seconds*}

no fhrp delay {[**minimum**] [**reload**] *seconds*}

構文の説明

minimum	（任意）インターフェイスが使用可能になった後の遅延時間を設定します。
reload	（任意）デバイスのリロード後の遅延時間を設定します。
seconds	秒単位の遅延時間。範囲は 0 ～ 3600 です。

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（config-if）

次に、FHRP クライアントの初期化の遅延期間を指定する例を示します。

```
Device(config-if)# fhrp delay minimum 90
```

関連コマンド

コマンド	説明
show fhrp	ファースト ホップ冗長性プロトコル（FHRP）の情報を表示します。

fhrp version vrrp v3

Virtual Router Redundancy Protocol バージョン 3（VRRPv3）と Virtual Router Redundancy Service（VRRS）をデバイスで有効にするには、グローバル コンフィギュレーション モードで **fhrpversionvrrpv3** コマンドを使用します。VRRPv3 と VRRS の設定機能をデバイスで無効にするには、このコマンドの **no** 形式を使用します。

fhrp version vrrp v3

no fhrp version vrrp v3

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。

コマンド デフォルト

VRRPv3 と VRRS 設定はデバイスで有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

使用上のガイドライン

VRRPv3 が使用中の場合、VRRP バージョン 2（VRRPv2）は使用できません。

次の例では、トラッキング プロセスは、VRRPv3 グループを使用して IPv6 オブジェクトの状態を追跡するように設定されています。ギガビット イーサネット インターフェイス 0/0/0 の VRRP は、VRRPv3 グループで IPv6 オブジェクトに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス VRRPv3 の IPv6 オブジェクト ステートがダウンになると、VRRP グループのプライオリティは 20 だけ引き下げられます。

```
Device(config)# fhrp version vrrp v3
```

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

関連コマンド

コマンド	説明
track（**VRRP**）	VRRPv3 グループを使用したオブジェクトの追跡を有効にします。

glbp authentication

Gateway Load Balancing Protocol（GLBP）の認証文字列を設定するには、インターフェイス コンフィギュレーション モードで **glbpauthentication** 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。

glbp *group-number***authentication** {**text** *string*| **md5** {**key-string** [**0**| **7**] *key*| **key-chain** *name-of-chain*}}

no glbp *group-number* **authentication** {**text** *string*| **md5** {**key-string** [**0**| **7**] *key*| **key-chain** *name-of-chain*}}

構文の説明

group-number	0 ～ 1023 の範囲の GLBP グループ番号。
text*string*	認証ストリングを指定します。コマンドとテキストを合わせた文字数が 255 文字を超えないようにします。
md5	Message Digest 5（MD5）認証。
key-string*key*	MD5 認証の秘密キーを指定します。キー ストリングは、100 文字の長さを超えることはできません。少なくとも 16 文字使用することを推奨します。
0	（任意）非暗号化キー。プレフィックスが指定されていない場合、キーは暗号化されません。
7	（任意）暗号化キー。
key-chain*name-of-chain*	認証キーのグループを指定します。

コマンド デフォルト

GLBP メッセージの認証は発生しません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

使用上のガイドライン

同じGLBPグループのメンバーとして設定されているすべてのデバイスで同じ認証方式を設定し、確実に相互運用できるようにする必要があります。デバイスは、誤った認証情報を含むすべてのGLBP メッセージを無視します。

パスワード暗号化が**servicepassword-encryption** コマンドで設定されると、ソフトウェアは、キー文字列を暗号化されたテキストとして設定に保存します。

次に、グループ10のGLBPデバイスの相互運用を許可するために必要な認証文字列としてstringxyzを設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 authentication text stringxyz
```

次に、GLBP がキー チェーン「AuthenticateGLBP」を照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得する例を示します。

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

関連コマンド

コマンド	説明
glbpip	GLBP をイネーブルにします。

glbp forwarder preempt

現在のアクティブ仮想フォワーダ（AVF）がその低い重み付けしきい値を下回った場合に、デバイスが Gateway Load Balancing Protocol（GLBP）グループの AVF として引き継がれ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 **glbpforwarderpreempt** 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。

glbp *group* **forwarder preempt** [**delay minimum** *seconds*]

no glbp *group* **forwarder preempt** [**delay minimum**]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。

delayminimum*seconds*	（任意）デバイスが AVF のロールを引き継ぐ前に遅延する最小秒数を指定します。範囲は 0 ～ 3600 秒です。デフォルトの遅延時間は 30 秒です。

コマンド デフォルト

フォワーダ強制排除は、30 秒のデフォルト遅延で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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

次に、現在の AVF がその低い重み付けしきい値を下回った場合に、デバイスが現在の AVF をプリエンプション処理するように設定する例を示します。デバイスが現在の AVF をプリエンプション処理した場合、デバイスは AVF の役割を引き継ぐ前に 60 秒間待ちます。

```
Device(config-if)# glbp 10 forwarder preempt delay minimum 60
```

関連コマンド

コマンド	説明
glbpip	GLBP をイネーブルにします。

glbp ip

Gateway Load Balancing Protocol（GLBP）を有効化するには、インターフェイス コンフィギュレーション モードで **glbpip** コマンドを使用します。GLBP を無効にするには、このコマンドの **no** 形式を使用します。

glbp *group* **ip** [*ip-address* **[secondary]**]

no glbp *group* **ip** [*ip-address* **[secondary]**]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
ip-address	（任意）GLBP グループの仮想 IP アドレス。この IP アドレスはインターフェイス IP アドレスと同じサブネット内になければなりません。
secondary	（任意）IP アドレスがセカンダリ GLBP 仮想アドレスであることを示します。

コマンド デフォルト

GLBP はデフォルトでは無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

glbpip コマンドを実行すると、設定されたインターフェイスで GLBP が有効になります。指定されている IP アドレスがある場合、そのアドレスが GLBP グループの指定仮想 IP アドレスとして使用されます。指定されている IP アドレスがない場合、指定アドレスは、同じ GLBP グループに属するよう設定された別のデバイスから取得されます。GLBP がアクティブ仮想ゲートウェイ（AVG）を選択する場合、ケーブル上の少なくとも 1 つのデバイスが指定アドレスで設定されている必要があります。デバイスは、GLBP ゲートウェイまたはフォワーダの権限を引き受ける前に、GLBP グループの仮想 IP アドレスで設定されているか、そのアドレスを取得している必要があります。AVG の指定アドレスを設定すると、常に使用されている指定アドレスが上書きされます。

glbpip コマンドがインターフェイスで有効になっている場合、プロキシの Address Resolution Protocol（ARP）要求の処理方法が変更されます（プロキシ ARP が無効になっていない場合）。ARP 要求はホストにより送信され、IP アドレスが MAC アドレスにマッピングされます。GLBP ゲートウェイは、ARP 要求を代行受信し、接続先ノードの代わりに ARP に応答します。GLBP グループのフォワーダがアクティブである場合、プロキシ ARP 要求への応答には、グループ内の最初のアク

ティブ フォワーダの MAC アドレスが使用されます。アクティブなフォワーダがない場合、プロキシ ARP 要求は停止されます。

次の例では、GigabitEthernet インターフェイス 1/0/1 上の グループ 10 の GLBP を有効にします。GLBP グループで使用される仮想 IP アドレスは、10.21.8.10 に設定されます。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

関連コマンド

コマンド	説明
showglbp	GLBP の情報を表示します。

glbp load-balancing

Gateway Load Balancing Protocol（GLBP）のアクティブ仮想ゲートウェイ（AVG）で使用されるロード バランシング方式を指定するには、インターフェイス コンフィギュレーション モードで **glbpload-balancing** コマンドを使用します。ロード バランシングを無効にするには、このコマンドの **no** 形式を使用します。

glbp *group* **load-balancing** [**host-dependent**| **round-robin**| **weighted**]

no glbp *group* **load-balancing**

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
host-dependent	（任意）ホストの MAC アドレスに基づくロードバランシング方式（GLBP グループ メンバーの数を一定に保ったまま、特定のホストに常に同じフォワーダが使用される）を指定します。
round-robin	（任意）各仮想フォワーダが仮想 IP アドレスのアドレス解決応答に含まれるようなロードバランシング方式を指定します。この方式がデフォルトです。
weighted	（任意）ゲートウェイによってアドバタイズされる重み値に基づくロードバランシング方式を指定します。

コマンド モード

ラウンドロビン方式がデフォルトです。ョン（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

各ホストが常に同じデバイスを使用する必要がある場合は、ホスト依存方式の GLBP ロード バランシングを使用します。GLBP グループ内のデバイスの転送能力が異なるために不均等なロード バランシングを必要とする場合は、重み値方式の GLBP ロード バランシングを使用します。

次に、GLBP グループ 10 の AVG に設定されたホスト依存的な GLBP ロード バランシングの例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip 10.21.8.10
Device(config-if)# glbp 10 load-balancing host-dependent
```

関連コマンド

コマンド	説明
showglbp	GLBP の情報を表示します。

glbp name

Gateway Load Balancing Protocol（GLBP）グループに名前を割り当てて IP 冗長性を有効にするには、インターフェイス コンフィギュレーション モードで **glbpname** コマンドを使用します。グループの IP 冗長性を無効にするには、このコマンドの **no** 形式を使用します。

glbp *group-number* **name** *group-name*

no glbp *group-number* **name** *group-name*

構文の説明

group-number	GLBP グループ番号。指定できる値の範囲は 0 ～ 1023 です。
group-name	文字列で指定された GLBP グループ名。文字数は最大で 255 です。

コマンド デフォルト

グループの IP 冗長性は無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

冗長クライアントと GLBP グループを接続できるように、GLBP 冗長クライアントに同じ GLBP グループ名を設定する必要があります。

次に、GLBP グループ 10 に abccomp 名を割り当てる例を示します。

```
Device(config-if)# glbp 10 name abccomp
```

関連コマンド

コマンド	説明
glbpauthentication	GLBP に認証ストリングを設定します。
glbpforwarderpreempt	デバイスの優先順位が現在の AVF より高い場合、デバイスが GLBP グループの AVF として引き継がれるように設定します。
glbpip	GLBP を有効にします。
glbpload-balancing	GLBP のアクティブ仮想ゲートウェイ（AVG）によって使用されるロードバランシング方式を指定します。
glbppreempt	ゲートウェイの優先順位が現在の AVG より高い場合、ゲートウェイが GLBP グループの AVG として引き継がれるように設定します。

コマンド	説明
glbppriority	GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。
glbptimers	GLBP ゲートウェイによって送信される hello パケット間の時間、および仮想ゲートウェイと仮想フォワーダの情報が有効と見なされる時間を設定します。
glbptimersredirect	GLBP グループの AVG がセカンダリ AVF にクライアントをリダイレクトし続ける時間を設定します。
glbpweighting	GLBP ゲートウェイの最初の重み値を指定します。
glbpweightingtrack	GLBP の重み値の変更がトラッキングされるオブジェクトの可用性に基づいているトラッキング オブジェクトを指定します。
showglbp	GLBP の情報を表示します。
track	GLBP 重み付けの変更がインターフェイスの状態に基づいている場合、インターフェイスをトラッキングするように設定します。

glbp preempt

現在のアクティブ仮想ゲートウェイ（AVG）よりも優先順位の高いゲートウェイがある場合、そのゲートウェイが Gateway Load Balancing Protocol（GLBP）グループの AVG を引き継ぐ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 **glbppreempt** 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。

glbp *group* **preempt** [**delay minimum** *seconds*]

no glbp *group* **preempt** [**delay minimum**]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。

delayminimum*seconds*	（任意）デバイスが AVG の役割を引き継ぐ前に遅延する最小秒数を指定します。範囲は 0 ～ 3600 秒です。デフォルトの遅延時間は 30 秒です。

コマンド デフォルト

現在の AVG よりも優先順位の高い GLBP ゲートウェイが、AVG の役割を引き継ぐことはできません。デフォルトの遅延時間は 30 秒です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

次に、デバイスの優先順位が 254 で、現在の AVG よりも優先順位が高い場合に、そのデバイスが現在の AVG をプリエンプション処理するように設定する例を示します。デバイスが現在の AVG をプリエンプション処理する場合、デバイスは、AVG の役割を引き継ぐ前に 60 秒間待ちます。

```
Device(config-if)# glbp 10 preempt delay minimum 60
Device(config-if)# glbp 10 priority 254
```

関連コマンド

コマンド	説明
glbpip	GLBP をイネーブルにします。
glbppriority	GLBP グループ内のデバイスの優先度レベルを設定します。

glbp priority

Gateway Load Balancing Protocol（GLBP）グループ内のゲートウェイの優先度レベルを設定するには、インターフェイス コンフィギュレーション モードで **glbppriority** コマンドを使用します。ゲートウェイの優先度レベルを削除するには、このコマンドの **no** 形式を使用します。

glbp *group* **priority** *level*

no glbp *group* **priority** *level*

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
level	GLBP グループ内のゲートウェイのプライオリティ。範囲は 1 ～ 255 です。デフォルトは 100 です。

コマンド デフォルト

GLBP 仮想ゲートウェイのプリエンプション スキームは無効になっています。

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（config-if）

使用上のガイドライン

アクティブ仮想ゲートウェイ（AVG）になる仮想ゲートウェイを制御するには、このコマンドを使用します。異なる複数の仮想ゲートウェイの優先順位を比較した後、優先順位の数値が高いゲートウェイが AVG として選択されます。2 つの仮想ゲートウェイの優先順位が等しい場合、優先順位の高い IP アドレスが選択されます。

次に、仮想ゲートウェイを 254 の優先順位に設定する例を示します。

```
Device(config-if)# glbp 10 priority 254
```

関連コマンド

コマンド	説明
glbpip	GLBP をイネーブルにします。
glbppreempt	現在の AVG よりも優先順位の高いデバイスがある場合、そのデバイスが GLBP グループの AVG を引き継ぐように設定します。

glbp timers

Gateway Load Balancing Protocol（GLBP）ゲートウェイにより送信される hello パケットの時間間隔、および仮想ゲートウェイと仮想フォワーダ情報が有効と見なされる時間を設定するには、インターフェイス コンフィギュレーション モードで **glbptimers** コマンドを使用します。タイマー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。

glbp *group* **timers** {*hellotime*{*holdtime* | **msec** *holdtime*} | **msec** { *holdtime* | **msec** *holdtime*} | **redirect** *time-interval-to-redirect* | *timeout*}

no glbp *group* **timers** {*hellotime*{*holdtime* | **msec** *holdtime*} | **msec** { *holdtime* | **msec** *holdtime*} | **redirect** *time-interval-to-redirect* | *timeout*}

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
msec	（任意）下記の（*hellotime* または *holdtime*）引数値をミリ秒で表すように指定します。
hellotime	hello 間隔デフォルトは 3 秒（3000 ミリ秒）です。
holdtime	helloパケットに含まれる仮想ゲートウェイおよび仮想フォワーダの情報が無効と見なされるまでの時間。デフォルトは10秒（10,000ミリ秒）です。
redirect	Gateway Load Balancing Protocol（GLBP）グループのアクティブ仮想ゲートウェイ（AVG）が継続してクライアントをセカンダリ アクティブ仮想フォワーダ（AVF）にリダイレクトする時間間隔を指定します。

time-interval-to-redirect	リダイレクト タイマーの間隔は、0 ～ 3600 秒の範囲内です。デフォルトは600秒（10分）です。 （注） *time-interval-to-redirect* 引数のゼロ（0）値は、指定できる値の範囲から除外することはできません。Cisco IOS ソフトウェアの事前設定でゼロ（0）値を使用しているため、アップグレードに悪影響を及ぼすことになります。ただし、ゼロ（0）値に設定することは推奨しません。 *time-interval-to-redirect* にこの値を使用すると、リダイレクト タイマーが期限切れになりません。リダイレクト タイマーが期限切れにならず、デバイスに障害が発生すると、新しいホストがバックアップへリダイレクトされずに、障害が発生したデバイスに引き続き割り当てられます。
timeout	セカンダリ仮想フォワーダが使用できなくなるまでの 600 秒から 64,800 秒の範囲の時間間隔。デフォルトは 14,400 秒（4 時間）です。

コマンド デフォルト

GLBP タイマーはデフォルト値に設定されています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

タイマー値が設定されていないデバイスは、アクティブ仮想ゲートウェイ（AVG）からタイマー値を取得できます。AVG 上に設定されているタイマーは、他のすべてのタイマー設定を常に上書

きします。GLBP グループ内のすべてのデバイスが同じタイマー値を使用するようにしてください。GLBP ゲートウェイが hello メッセージを送信した場合、その情報は 1 ホールドタイムの間有効と見なされます。通常、保留時間は hello タイムの値の 3 倍より大きくします（*holdtime* > 3 * *hellotime*）。保留時間の値の範囲によって、hello タイムより大きい保留時間が強制されます。

次に、GigabitEthernet インターフェイス 1/0/1 の GLBP グループ 10 の hello パケットの間隔を 5 秒に設定し、仮想ゲートウェイとバーチャル フォワーダの情報が無効と見なされる時間を 18 秒に設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip
Device(config-if)# glbp 10 timers 5 18
```

関連コマンド

コマンド	説明
glbpip	GLBP を有効にします。
showglbp	GLBP の情報を表示します。

glbp weighting

Gateway Load Balancing Protocol（GLBP）ゲートウェイの初期重み値を指定するには、インターフェイス コンフィギュレーション モードで **glbpweighting** 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。

glbp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]

no glbp *group* **weighting**

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
maximum	1 ～ 254 の範囲の最大重み値。デフォルト値は 100 です。
lower*lower*	（任意）1 から指定された最大重み値までの範囲で重み値の下限を指定します。デフォルト値は 1 です。
upper*upper*	（任意）重み値の下限から最大重み値までの範囲で重み値の上限を指定します。デフォルト値は指定された最大重み値です。

コマンド デフォルト

デフォルトのゲートウェイ重み値は 100 で、デフォルトの下限重み値は 1 です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

仮想ゲートウェイの重み値は、ゲートウェイの転送能力の指標です。デバイス上の追跡対象インターフェイスに障害が発生し、そのデバイスの重み値が最大値から下限しきい値を下回るまで減ると、デバイスは仮想フォワーダとしての役割を放棄します。デバイスの重み値が上限しきい値を上回るまで増えると、デバイスは仮想フォワーダのアクティブな役割を再開できます。

追跡対象となるインターフェイスのパラメータを設定するには、**glbpweightingtrack** and **track** コマンドを使用します。デバイスのインターフェイスがダウンすると、デバイスの重み値が指定された値まで減少する場合があります。

次に、GLBP グループ 10 のゲートウェイの重み値を、重み値の下限を 95 に、重み値の上限を105 に、最大値を 110 に設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
```

関連コマンド

コマンド	説明
glbpweightingtrack	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。
track	追跡対象インターフェイスを設定します。

glbp weighting track

トラッキング対象オブジェクトの可用性に基づいてGateway Load Balancing Protocol（GLBP）の重み値が増減するようにトラッキング対象オブジェクトを指定するには、インターフェイス コンフィギュレーション モードで **glbpweightingtrack** コマンドを指定します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

glbp *group* **weighting track** *object-number* [**decrement** *value*]

no glbp *group* **weighting track** *object-number* [**decrement** *value*]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
object-number	トラッキング対象オブジェクトを表すオブジェクト番号。有効な範囲は1～1000です。トラッキング対象オブジェクトを設定するには、**track** コマンドを使用します。
decrement*value*	（任意）インターフェイスがダウン（または復旧）したときにデバイスのGLBPの重み値を減らす（または増やす）量を指定します。値の範囲は 1 ～ 254 です。デフォルト値は 10 です。

コマンド デフォルト

GLBP の重み値の変更時に、オブジェクトはトラッキングされません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

このコマンドを使用して、GLBP ゲートウェイの重み値とゲートウェイ インターフェイスの可用性を関連付けます。これは、GLBP に設定されてないインターフェイスをトラッキングする場合に便利です。

トラッキング対象のインターフェイスがダウンすると、GLBP ゲートウェイの重み値は 10 減少します。インターフェイスがトラッキングされない場合、インターフェイスの状態の変化は GLBP ゲートウェイの重み値に影響しません。GLBP グループごとに、トラッキング対象インターフェイスの個別のリストを設定できます。

オプションの *value* 引数は、トラッキング対象のインターフェイスがダウンした場合に GLBP ゲートウェイの重み値をどれだけデクリメントするかを指定します。トラッキング対象インターフェイスが稼働状態に戻ると、重み値は同じ分だけ増加します。

複数のトラッキング対象インターフェイスがダウンすると、それぞれに設定されている重みの減分値が累計されます。

各インターフェイスをトラッキング対象に設定するには、**track** コマンドを使用します。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できるかどうかは、使用可能な CPU によって異なります。特定のサイトトラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

この例では、GigabitEthernet インターフェイス 1/0/1 で、番号の 1 と 2 で表される 2 つのインターフェイスがトラッキングされることを示します。インターフェイス 1 がダウンすると、GLBP ゲートウェイ重み付けがデフォルト値の 10 だけ減算されます。インターフェイス 2 がダウンすると、GLBP ゲートウェイ重み付けが 5 だけ減算されます。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2 decrement 5
```

関連コマンド

コマンド	説明
glbpweighting	GLBP ゲートウェイの初期重み値を指定します。
track	追跡対象インターフェイスを設定します。

ip address dhcp

DHCP からインターフェイスの IP 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 **ipaddressdhcp** コマンドを使用します。取得されたいずれかのアドレスを削除するには、このコマンドの **no** 形式を使用します。

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

構文の説明

client-id	（任意）クライアント ID を指定します。デフォルトでは、クライアント識別子は ASCII 値です。**client-id***interface-typenumber* オプションは、クライアント識別子を、指定されたインターフェイスの 16 進数 MAC アドレスに設定します。
interface-type	（任意）インターフェイス タイプ。詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
number	（任意）インターフェイスまたはサブインターフェイスの番号です。ネットワーキング デバイスに対する番号付け構文の詳細については、疑問符（?）のオンライン ヘルプ機能を使用してください。
hostname	（任意）ホスト名を指定します。
hostname	（任意）ホスト名を DHCP オプション 12 フィールドに配置します。この名前は、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ホスト名と同じにする必要はありません。

コマンド デフォルト

ホスト名は、デバイスのグローバル コンフィギュレーション ホスト名です。クライアント識別子は ASCII 値です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.1(2)T	このコマンドが導入されました。
12.1(3)T	このコマンドが変更されました。**client-id** キーワードと *interface-typenumber* 引数が追加されました。
12.2(3)	このコマンドが変更されました。**hostname** キーワードと *hostname* 引数が追加されました。**client-id***interface-typenumber* オプションの動作は変更されています。詳細については、「使用上のガイドライン」セクションを参照してください。
12.2(8)T	このコマンドが変更されました。このコマンドは、ATM（PPPoA）インターフェイスおよび特定の ATM インターフェイスでの PPP の使用のために展開されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
15.1(3)T	このコマンドが変更されました。トンネル インターフェイスでのサポートが提供されていました。

使用上のガイドライン

（注） Cisco IOS リリース 12.2(8) T よりも前には、**ipaddressdhcp** コマンドはイーサネット インターフェイスのみで使用が可能でした。

ipaddressdhcp 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 IP アドレスを動的に学習できます。これはインターネット サービス プロバイダー（ISP）に動的に接続するイーサネットインターフェイスで特に役立ちます。このインターフェイスにダイナミックアドレスを割り当てると、同インターフェイスを使用して、Cisco IOS ネットワーク アドレス変換（NAT ）のポート アドレス変換（PAT）で、デバイスに接続済みの個別に処理されたネットワークにインターネット アクセスを提供できます。

また **ipaddressdhcp** コマンドは、ATM ポイントツーポイント インターフェイスと連動し、どのカプセル化方式でも受け入れます。ただし、ATM マルチポイント インターフェイスの場合、**protocolipinarp** インターフェイス コンフィギュレーション コマンドで Inverse ARP を指定し、aa15snap カプセル化タイプのみを使用する必要があります。

一部の ISP の場合、DHCPDISCOVER メッセージに、特定のホスト名と、インターフェイスの MAC アドレスであるクライアント識別子を含める必要があります。**ipaddressdhcpclient-id***interface-typenumber***hostname***hostname* が使用される最も一般的な状況は、このコマンドが設定されるイーサネット インターフェイスが *interface-type* で、ISP によって入力されるホスト名が *interface-typenumber* の場合です。

クライアント識別子（DHCP オプション 61）には、16 進数または ASCII 値を使用できます。デフォルトでは、クライアント識別子は ASCII 値です。**client-id***interface-typenumber* オプションは、デフォルトの値を上書きし、指定されたインターフェイスの 16 進数 MAC アドレスの使用を強制します。

（注） Cisco IOS リリース 12.1(3)T から 12.2(3) までのリリースでは、**client-id** オプション キーワードは、クライアント識別子の ASCII 固定値の変更を許可します。リリース 12.2(3) 以降、**client-id** オプション キーワードは、クライアント識別子として指定されたインターフェイスの 16 進数 MAC アドレスの使用を強制します。

DHCP サーバから IP アドレスを取得するようシスコ デバイスが設定されている場合、デバイスは、ネットワークの DHCP サーバにデバイスに関する情報を提供する DHCPDISCOVER メッセージを送信します。

ipaddressdhcp コマンドを使用する場合、オプション キーワードの有無にかかわらず、DHCP オプション 12 フィールド（ホスト名オプション）が DISCOVER メッセージに含められます。デフォルトでは、オプション 12 で指定されたホスト名は、デバイスのグローバル コンフィギュレーション ホスト名になります。とはいえ、**ipaddressdhcphostname***hostname* コマンドを使用して、デバイスのグローバル コンフィギュレーション ホスト名ではない別の名前を DHCP オプション 12 フィールドに入力することもできます。

noipaddressdhcp コマンドは、取得済みの IP アドレスを削除して、DHCPRELEASE メッセージを送信します。

DHCP サーバで必要なものを判別するため、さまざまな設定を試行しなければならない場合があります。下の表に、使用可能なコンフィギュレーション方式と、各方式の DISCOVER メッセージに含まれる情報を示します。

表 *19*：コンフィギュレーション方式と生成される *DISCOVER* メッセージの内容

コンフィギュレーション方式	DISCOVER メッセージの内容
ipaddressdhcp	DISCOVER メッセージのクライアント ID フィールドには「cisco- *mac-address* -Eth1」が含まれます。*mac-address* は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドのデバイスのデフォルト ホスト名を含んでいます。

コンフィギュレーション方式	DISCOVER メッセージの内容
ipaddressdhcphostname*hostname*	DISCOVERメッセージのクライアントIDフィールドには「cisco- *mac-address* -Eth1」が含まれます。*mac-address* は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドの *hostname* を含んでいます。
ipaddressdhcpclient-idethernet1	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドにデバイスのデフォルト ホスト名を含んでいます。
ipaddressdhcpclient-idethernet1hostname*hostname*	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドに *hostname* を含んでいます。

次の例では、**ipaddressdhcp** コマンドがイーサネット インターフェイス 1 に入力されます。次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドの「cisco- *mac-address* -Eth1」と、オプション 12 フィールドの値 abc が含まれます。

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp
```

次の例のように設定されたデバイスによって送信されたDISCOVERメッセージには、クライアント ID フィールドの「cisco- mac-address -Eth1」と、オプション 12 フィールドの値 def が含まれます。

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp hostname def
```

次の例のように設定されたデバイスによって送信されたDISCOVERメッセージには、クライアント ID フィールドの イーサネット インターフェイス 1 の MAC アドレスと、オプション 12 フィールドの値 abc が含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1
```

次の例のように設定されたデバイスによって送信されたDISCOVERメッセージには、クライアント ID フィールドの イーサネット インターフェイス 1 の MAC アドレスと、オプション 12 フィールドの値 def が含まれます。

```
hostname abc
!
```

```
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1 hostname def
```

関連コマンド

コマンド	説明
ipdhcppool	Cisco IOS DHCP サーバに DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。

ip address pool (DHCP)

Dynamic Host Configuration Protocol（DHCP）に IP Control Protocol （IPCP）ネゴシエーションからサブネットが入力されるときに、インターフェイスの IP アドレスが自動設定されるようにするには、インターフェイス コンフィギュレーション モードで **ipaddresspool** コマンドを使用します。インターフェイスの IP アドレスの自動設定を無効にするには、このコマンドの **no** 形式を使用します。

ip address pool *name*

no ip address pool

構文の説明

name	DHCP プールの名前。インターフェイスの IP アドレスは、*name* で指定された DHCP プールから自動設定されます。

コマンド デフォルト

IP アドレスのプーリングは無効になっています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(8)T	このコマンドが導入されました。

使用上のガイドライン

デバイスのDHCPプールによって処理する必要のある LAN に接続されている DHCP クライアントが存在する場合、このコマンドを使用して LAN インターフェイスの IP アドレスを自動設定します。DHCP プールは、IPCP サブネット ネゴシエーションによってサブネットを動的に取得します。

次の例では、GigabitEthernet インターフェイス 1/0/1 の IP アドレスが abc という名前のアドレスプールから自動設定されるように指定します。

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

関連コマンド

コマンド	説明
showipinterface	IP用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

ip address

インターフェイスのプライマリまたはセカンダリ IP アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ipaddress** コマンドを使用します。IP アドレスを削除するか、IP 処理を無効にするには、このコマンドの no 形式を使用します。

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

構文の説明

ip-address	[IP Address]。
mask	関連する IP サブネットのマスク。

secondary	（任意）設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 （注） セカンダリ アドレスが **vrf**のキーワードでの VRF テーブルの設定に使用される場合には、**VRF** キーワードも指定する必要があります。
vrf	（任意）VRF テーブルの名前*vrf-name* 引数は、入力インターフェイスの VRF 名を指定します。

コマンド デフォルト

IP アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	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、1 つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。Cisco IOS ソフトウェアにより生成されるパケットは、必ずプライマリ IP アドレスを使用します。そのため、セグメントのすべてのデバイスとアクセスサーバは、同じプライマリ ネットワーク番号を共有する必要があります。

ホストは、Internet Control Message Protocol（ICMP）マスク要求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。デバイスは、ICMP マスク応答メッセージでこの要求に応答できます。

noipaddress コマンドを使用して IP アドレスを削除することにより、特定のインターフェイス上の IP 処理を無効にできます。ソフトウェアが、その IP アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラー メッセージを出力します。

オプションの **secondary** キーワードを使用すると、セカンダリ アドレスを無制限に指定できます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストおよび Address Resolution Protocol（ARP）要求は、IP ルーティング テーブルのインターフェイス ルートのように、正しく処理されます。

セカンダリ IP アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワーク セグメントに十分なホスト アドレスがない場合。たとえば、サブネット化により、論理サブネットあたり最大254のホストを使用できますが、1つの物理サブネットでは、300のホスト アドレスが必要になります。デバイスまたはアクセス サーバでセカンダリ IP アドレスを使用すると、2 つの論理サブネットで 1 つの物理サブネットを使用できます。
- レベル 2 ブリッジを使用して構築された旧式ネットワークがたくさんある場合。セカンダリ アドレスは、慎重に使用することで、サブネット化されたデバイスベース ネットワークへの移行に役立ちます。旧式のブリッジセグメントのデバイスでは、そのセグメントに複数のサブネットがあることを簡単に認識させることができます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。サブネットが使用中の場合、この状況は許可されません。このような場合、最初のネットワークは、セカンダリ アドレスを使用している2番目のネットワークの上に拡張されます。つまり、上の階層となります。

（注） ネットワーク セグメント上のすべてのデバイスがセカンダリ 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。

（注） Open Shortest Path First（OSPF）アルゴリズムを使用してルーティングする場合は、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 アドレスと同じ OSPF エリアにあることを確認してください。

インターフェイスで IP を透過的にブリッジする前に、次の手順を実行する必要があります。

- IP ルーティングを無効にします（**noiprouting** コマンドを指定します）。
- インターフェイスをブリッジ グループに追加して、**bridge-group** コマンドを参照してください。

インターフェイスでIPのルーティングと透過的なブリッジングを同時に実行するには、**bridgecrb** コマンドを参照してください。

次の例では、192.108.1.27 が プライマリ アドレスで、192.31.7.17 と 192.31.8.17 が GigabitEthernet インターフェイス 1/0/1のセカンダリ アドレスです。

```
interface GigabitEthernet 1/0/1
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
```

関連コマンド

コマンド	説明
matchiproute-source	送信元 IP アドレスを、VRF で接続されたルートに基づいて設定された必要なルートマップに一致するように指定します。
route-map	1 つのルーティング プロトコルから他のルーティング プロトコルへのルートを再配布するか、またはポリシー ルーティングを有効にするための条件を定義します。
setvrf	ポリシーベース ルーティング VRF の選択のために、ルート マップ内で VPN VRF 選択を有効にします。
showiparp	SLIP アドレスが固定 ARP テーブル エントリとして表示される ARP キャッシュを表示します。
showipinterface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。
showroute-map	静的ルート マップとダイナミック ルート マップを表示します。

ip nhrp map

ノンブロードキャスト マルチアクセス（NBMA）ネットワークに接続された IP 宛先の IP と NBMA 間のアドレス マッピングをスタティックに設定するには、インターフェイス コンフィギュレーション モードで **ipnhrpmap** コマンドを使用します。Next Hop Resolution Protocol（NHRP）キャッシュからスタティック 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 nhrp map *ip-address*{*ip-nbma-address*| *destination-mask*[*ip-nbma-address*| *ipv6-nbma-address*] | *ipv6-nbma-address*}

noip nhrp map *ip-address*{*ip-nbma-address*| *destination-mask*[*ip-nbma-address*| *ipv6-nbma-address*] | *ipv6-nbma-address*}

構文の説明

ip-address	NBMA ネットワーク経由で到達可能な宛先の IP アドレス。このアドレスは、NBMA アドレスにマッピングされます。
ip-nbma-address	NBMA ネットワーク経由で直接到達可能な NBMA アドレス。アドレス形式はメディアによって異なります。たとえば、ATM にはネットワーク サービス アクセス ポイント（NSAP）アドレスがあり、イーサネットには MAC アドレスがあり、Switched Multimegabit Data Service（SMDS; スイッチド マルチメガビット データ サービス）には E.164 アドレスがあります。このアドレスは、IP アドレスにマッピングされます。
destination-mask	宛先アドレス マスク。
ipv6-nbma-address	IPv6 NBMA アドレス。 （注） この引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。

コマンド デフォルト

スタティック IP-to-NBMA キャッシュは存在しません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

Cisco IOS XE Denali 16.3.1 では、NHRP はハブ/スポーク間通信のみをサポートし、スポーク間通信はサポートされていません。

（注） Cisco IOS XE Denali 16.3.1 では、このコマンドは IPv4 のみをサポートします。*ipv6-nbma-address* 引数はスイッチで使用できますが、設定しても無効です。

ネクストホップ サーバに到達するには、少なくとも 1 つのスタティック マッピングを設定します。統計的に複数の IP-to-NBMA アドレス マッピングを設定するには、このコマンドを複数回設定します。

ルーティング プロトコル、Open Shortest Path First（OSPF）または Enhanced Interior Gateway Routing Protocol（EIGRP）を使用している場合は、トラフィックを許可するトンネルで、**ipospfnetworkpoint-to-multipoint** コマンド（OSPF がハブ/スポーク通信に使用されている場合）および **ipsplit-horizoneigrp** コマンド（EIGRP が使用されている場合）を設定します。

次に、マルチポイント トンネル ネットワーク内のこのステーションが 2 つのネクストホップ サーバ 10.0.0.1 と 10.0.1.3 によってサービス提供されるようにスタティックに設定する例を示します。10.0.0.1 の NBMA アドレスは 192.0.2.1 としてスタティックに設定され、10.0.1.3 の NBMA アドレスは 198.51.100.1 です。

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip nhrp nhs 10.0.0.1
Switch(config-if)# ip nhrp nhs 10.0.1.3
Switch(config-if)# ip nhrp map 10.0.0.1 192.0.2.1
Switch(config-if)# ip nhrp map 10.0.1.3 198.51.100.1
```

関連コマンド

コマンド	説明
clearipnhrp	NHRP キャッシュからすべてのダイナミック エントリを削除します。
debugnhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ipsplit-horizoneigrp	EIGRP スプリット ホライズンを有効にします。
ipospfnetworkpoint-to-multipoint	OSPF ネットワーク タイプをポイントツーマルチポイントに設定します。

ip nhrp map multicast

トンネル ネットワーク経由で送信されるブロードキャストまたはマルチキャスト パケットの宛先として使用されるノンブロードキャスト マルチアクセス（NBMA）アドレスを設定するには、イ

ンターフェイス コンフィギュレーション モードで **ipnhrpmapmulticast** コマンドを使用します。宛先を削除するには、このコマンドの **no** 形式を使用します。

ip nhrp map multicast {*ip-nbma-address*| *ipv6-nbma-address*| **dynamic**}

no ip nhrp map multicast {*ip-nbma-address*| *ipv6-nbma-address*| **dynamic**}

構文の説明

ip-nbma-address	NBMA ネットワーク経由で直接到達可能な NBMAアドレス。アドレス形式は、使用しているメディアによって異なります。
ipv6-nbma-address	IPv6 NBMA アドレス。 （注） この引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。
dynamic	ハブのクライアント登録から宛先をダイナミックに学習します。

コマンド デフォルト

NBMAアドレスは、ブロードキャストまたはマルチキャストパケットの宛先として設定されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

（注） Cisco IOS XE Denali 16.3.1 では、このコマンドはIPv4 のみをサポートします。*ipv6-nbma-address* 引数はスイッチで使用できますが、設定しても無効です。

このコマンドは、トンネル インターフェイスだけに適用されます。このコマンドは、基盤となるネットワークがIPマルチキャストをサポートしていない場合に、トンネル ネットワーク経由でブ

ロードキャストをサポートするために役立ちます。基盤となるネットワークがIPマルチキャストをサポートしている場合は、**tunneldestination** コマンドを使用して、トンネル ブロードキャストまたはマルチキャストを伝送するためのマルチキャスト宛先を設定する必要があります。

複数の NBMA アドレスが設定されている場合、システムはアドレスごとにブロードキャスト パケットを複製します。

次に、パケットが 10.255.255.255 に送信される場合に、宛先 10.0.0.1 と 10.0.0.2 に対してパケットが複製される例を示します。

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip address 10.0.0.3 255.0.0.0
Switch(config-if)# ip nhrp map multicast 10.0.0.1
Switch(config-if)# ip nhrp map multicast 10.0.0.2
```

関連コマンド

コマンド	説明
debugnhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
tunneldestination	トンネル インターフェイスの宛先を指定します。

ip nhrp network-id

インターフェイスの Next Hop Resolution Protocol（NHRP）を有効にするには、インターフェイス コンフィギュレーション モードで **ipnhrpnetwork-id** コマンドを使用します。インターフェイスで NHRP を無効にするには、このコマンドの **no** 形式を使用します。

ip nhrp network-id *number*

no ip nhrp network-id [*number*]

構文の説明

number	ノンブロードキャスト マルチアクセス（NBMA）ネットワークからのグローバルに一意な 32 ビット ネットワーク識別子。範囲は 1 ～ 4294967295 です。

コマンド デフォルト

NHRP はインターフェイスで無効になっています（no config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

一般に、論理 NBMA ネットワーク内のすべての NHRP ステーションは、同じネットワーク ID を使用して設定する必要があります。

次に、インターフェイスで NHRP を有効にする例を示します。

```
Switch(config-if)# ip nhrp network-id 1
```

関連コマンド

コマンド	説明
clearipnhrp	NHRP キャッシュからすべてのダイナミック エントリを削除します。
debugnhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

ip nhrp nhs

1 つ以上の Next Hop Resolution Protocol（NHRP）サーバのアドレスを指定するには、インターフェイス コンフィギュレーション モードで **ipnhrpnhs** コマンドを使用します。アドレスを削除するには、このコマンドの **no** 形式を使用します。

ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address*| *FQDN-string*}] **[multicast]** [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value*| **dynamic nbma** {*nbma-address*| *FQDN-string*} **[multicast]** [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

no ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address*| *FQDN-string*}] **[multicast]** [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value*| **dynamic nbma** {*nbma-address*| *FQDN-string*} **[multicast]** [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

構文の説明

nhs-address	指定されているネクストホップ サーバのアドレス。
nbma	（任意）ノンブロードキャスト マルチアクセス（NBMA）アドレスまたは FQDN を指定します。
nbma-address	NBMA アドレス。
FQDN-string	ネクスト ホップ サーバ（NHS）の完全修飾ドメイン名（FQDN）文字列。
multicast	（任意）ブロードキャストおよびマルチキャストに NBMA マッピングを使用することを指定します。
priority*value*	（任意）ハブに優先順位を割り当てて、トンネルを確立するためにスポークがハブを選択する順序を制御します。指定できる範囲は 0 ～ 255 で、0 は最高の優先順位、255 は最低の優先順位です。
cluster*value*	（任意）NHS グループを指定します。範囲は 0 ～ 10 です。
max-connections*value*	アクティブにする必要がある各 NHS グループの NHS 要素の数を指定します。有効な範囲は 0 ～ 255 です。
dynamic	NHS プロトコル アドレスをダイナミックに学習するようにスポークを設定します。
fallback*seconds*	リカバリ時により優先順位の高い NHS にフォールバックする前にスポークが待機する必要のある期間を秒単位で指定します。

コマンド デフォルト

ネクストホップ サーバは明示的に設定されていないため、通常のネットワーク層のルーティング決定が NHRP トラフィックの転送に使用されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ネクストホップ サーバのアドレスとそれがサービスを提供するネットワークを指定するには、**ipnhrpnhs** コマンドを使用します。通常、NHRP は、ネットワーク層転送テーブルを使用して、NHRP パケットの転送方法を決定します。ネクストホップ サーバが設定されている場合は、これらのネクストホップ アドレスの方が、通常 NHRP トラフィック向けに使用されている転送パスより優先されます。

設定されたネクストホップ サーバに対して、同じ *nhs-address* 引数を指定して **ipnhrpnhs** コマンドを繰り返すことで、複数のネットワークを指定できます。

次に、NBMA と FQDN を使用してハブをスポークに登録する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

次に、目的の **max-connections** 値を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

次に、NHS フォールバック時間を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs fallback 25
```

次に、NHS 優先順位とグループ値を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

関連コマンド

コマンド	説明
ipnhrpmap	NBMA ネットワークに接続された IP 宛先の IP-to-NBMA アドレス マッピングをスタティックに設定します。
showipnhrp	NHRP マッピング情報を表示します。

key chain

ルーティング プロトコルの認証を有効にし、キー チェーン コンフィギュレーション モードを開始するのに必要な認証キー チェーンを定義するには、グローバル コンフィギュレーション モードで **keychain** コマンドを使用します。キー チェーンを削除するには、このコマンドの **no** 形式を使用します。

key chain *name-of-chain*

no key chain *name-of-chain*

構文の説明

name-of-chain	キー チェーンの名前。キー チェーンには、少なくとも 1 つのキーを含める必要がありますが、最大 2147483647 個のキーを含めることができます。

コマンド デフォルト

キー チェーンは存在しません。

コマンド モード

グローバル コンフィギュレーション（config）

使用上のガイドライン

認証を有効にするには、キーでキー チェーンを設定する必要があります。

複数のキーチェーンの識別が可能ですが、ルーティングプロトコルごとのインターフェイスごとに1つのキーチェーンを使用することを推奨します。**keychain** コマンドを指定すると、キーチェーン コンフィギュレーション モードが開始されます。

次に、キー チェーンを指定する例を示します。

```
Device(config-keychain-key)# key-string chestnut
```

関連コマンド

コマンド	説明
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
key	キー チェーンの認証キーを識別します。
key-string(authentication)	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
showkeychain	認証キーの情報を表示します。

key-string（認証）

キーに認証文字列を指定するには、キーチェーン キー コンフィギュレーション モードで **key-string**（認証）コマンドを使用します。認証文字列を削除するには、このコマンドの **no** 形式を使用します。

key-string key-string *text*

no key-string *text*

構文の説明

text	認証されるルーティング プロトコルを使用してパケットで送信および受信される必要のある認証文字列。文字列には、大文字小文字の英数字 1 ～ 80 文字を含めることができます。

コマンド デフォルト

キーの認証文字列は存在しません。

コマンド モード

キー チェーン キー コンフィギュレーション（config-keychain-key）

次に、キーの認証文字列を指定する例を示します。

```
Device(config-keychain-key)# key-string key1
```

関連コマンド

コマンド	説明
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
key	キー チェーンの認証キーを識別します。
keychain	ルーティングプロトコルの認証をイネーブルにするために必要な認証キーチェーンを定義します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
showkeychain	認証キーの情報を表示します。

key

キー チェーンの認証キーを識別するには、キー チェーン コンフィギュレーション モードで **key** コマンドを使用します。キー チェーンからキーを削除するには、このコマンドの **no** 形式を使用します。

key *key-id*

no key *key-id*

構文の説明

key-id	キーチェーンの認証キーの識別番号。キーの範囲は 0 ～ 2147483647 です。キーの ID 番号は連続している必要はありません。

コマンド デフォルト

キー チェーンにキーは存在しません。

コマンド モード

キー チェーン コンフィギュレーション（config-keychain）

コマンド履歴

リリース	変更内容
11.1	このコマンドが導入されました。
12.4(6)T	IPv6 のサポートが追加されました。
12.2(33)SRB	このコマンドが、Cisco IOS Release 12.2(33)SRB に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の12.2SXリリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

キー チェーンに複数のキーを設定し、**accept-lifetime** および **send-lifetime** キー チェーン キー コマンド設定に基づいてキーが将来無効になるように、ソフトウェアがキーを配列できるようにすると便利です。

各キーには、ローカルに格納される独自のキー識別子があります。キーID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよびMessage Digest 5（MD5）認証キーが一意に識別されます。有効なキーの数にかかわらず、1 つの認証パケットのみが送信されます。ソフトウェアは、最小のキー識別番号の検索を開始し、最初の有効なキーを使用します。

最後のキーが期限切れになった場合、認証は続行されますが、エラー メッセージが生成されます。認証を無効にするには、手動で有効な最後のキーを削除する必要があります。

すべてのキーを削除するには、**nokeychain** コマンドを使用してキー チェーンを削除します。

次に、キーを指定してキー チェーンでの認証を確認する例を示します。

```
Device(config-keychain)# key 1
```

関連コマンド

コマンド	説明
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
keychain	ルーティング プロトコルの認証をイネーブルにするために必要な認証キーチェーンを定義します。

コマンド	説明
key-string(authentication)	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
showkeychain	認証キーの情報を表示します。

show glbp

Gateway Load Balancing Protocol（GLBP）情報を表示するには、特権 EXEC モードで **showglbp** コマンドを使用します。

capability [*interface-type interface-number*]*interface-type interface-number* [*group-number*] [*state*] **[brief]**

構文の説明

capability	（任意）GLBP 機能インターフェイスを表示します。
interface-typeinterface-number	（任意）出力を表示するインターフェイスのタイプおよび番号
group-number	（任意）0 ～ 1023 の範囲の GLBP グループ番号
state	（任意）次のいずれかの GLBP デバイスの状態：**active**、**disabled**、**init**、**listen**、**standby**
brief	（任意）1 行の出力で各仮想ゲートウェイまたは仮想フォワーダの要約を示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

デバイスの GLBP グループに関する情報を表示するには、**showglbp** コマンドを使用します。**brief** キーワードは、各仮想ゲートウェイまたは仮想フォワーダに関する情報を 1 行で表示します。**capability** キーワードは、すべての GLBP 対応インターフェイスを表示します。

次に、GLBP グループ 10 を表示する **showglbp** コマンドからの出力例を示します。

```
Device# show glbp GigabitEthernet 1/0/1 10
GigabitEthernet1/0/1 - Group 10
  State is Active
    1 state change, last state change 00:04:52
  Virtual IP address is 10.21.8.10
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.608 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption disabled
  Active is local
  Standby is unknown
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    ac7e.8a35.6364 (10.21.8.32) local
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:04:41
    MAC address is 0007.b400.0a01 (default)
    Owner ID is ac7e.8a35.6364
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *20*：*show glbp* フィールドの説明

フィールド	説明
GigabitEthernet 1/0/1 Group	インターフェイス タイプおよびインターフェイスの GLBP グループ番号。

フィールド	説明
State is	仮想ゲートウェイまたは仮想フォワーダのステート。仮想ゲートウェイの場合、ステートは次のいずれかになります。 • Active：ゲートウェイはアクティブ仮想ゲートウェイ（AVG）で、仮想 IP アドレスの Address Resolution Protocol（ARP）要求に応答します。 • Disabled：仮想 IP アドレスはまだ設定されていない、または学習されていませんが、別の GLBP 設定が存在します。 • Initial：仮想 IP アドレスは設定されている、または学習されていますが、仮想ゲートウェイの設定が完全ではありません。インターフェイスはアップ状態で、ルート IP に設定されている必要があります。インターフェイス IP アドレスが設定されている必要があります。 • Listen：仮想ゲートウェイは hello パケットを受信し、アクティブまたはスタンバイ仮想ゲートウェイが使用できなくなった場合に Speak ステートに変更できます。 • Speak：仮想ゲートウェイはアクティブまたはスタンバイ仮想ゲートウェイになろうとしています。 • Standby：ゲートウェイは次に AVG になる位置にいます。
Virtual IP address is	GLBP グループの仮想 IP アドレス。すべてのセカンダリ仮想 IP アドレスは、1 行ごとに表示されます。仮想 IP アドレスの 1 つが別のデバイスに設定されたアドレスと重複している場合、「duplicate」としてマークされます。重複アドレスは、デバイスが ARP キャッシュ エントリの保護に失敗したことを示します。

フィールド	説明
Hello time, hold time	Hello timeとは、helloパケット間の時間のことです（秒またはミリ秒単位）。Hold timeとは、他のデバイスがアクティブルータのダウンを宣言するまでの時間です（秒またはミリ秒単位）。GLBP グループのすべてのデバイスは、現在の AVG の hello 時間値と保留時間値を使用します。ローカルに設定された値が異なる場合、設定された値が hello 時間値と保留時間値の後ろのカッコ内に表示されます。
Next hello sent in	GLBPが次のhelloパケットを送信するまでの時間（秒またはミリ秒単位）。
Preemption	GLBPゲートウェイのプリエンプションがイネーブルであるかどうか。有効な場合、最小遅延は、優先順位の低いアクティブデバイスをプリエンプトするまで、優先順位の高いの非アクティブ デバイスが待つ時間です（秒単位）。 このフィールドも、GLBP フォワーダのプリエンプションを示すフォワーダ セクションの下に表示されます。
Active is	仮想ゲートウェイのアクティブ状態。値は「local」、「unknown」、またはIPアドレスです。アドレス（およびアドレスの有効期限）は、現在の AVG のアドレスです。 このフィールドも、現在の AVF のアドレスを示すフォワーダ セクションの下に表示されます。
Standby is	仮想ゲートウェイのスタンバイ状態。値は「local」、「unknown」、またはIPアドレスです。アドレス（およびアドレスの有効期限）は、スタンバイ ゲートウェイのアドレスです（ゲートウェイは次に AVG になります）。
Weighting	下限しきい値と上限しきい値のある初期重み値。
Track object	追跡対象オブジェクトのリストとそれらに対応する状態。
IP redundancy name is	GLBP グループの名前。

関連コマンド

コマンド	説明
glbpip	GLBP をイネーブルにします。
glbptimers	hello メッセージの間隔と、他のデバイスによってアクティブ GLBP デバイスのダウンが宣言されるまでの時間を設定します。
glbpweightingtrack	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。

show ip nhrp nhs

Next Hop Resolution Protocol（NHRP）ネクスト ホップ サーバ（NHS）情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip nhrp nhs** コマンドを使用します。

show ip nhrp nhs [*interface*] **[detail]** [**redundancy**[**cluster***number*| **preempted**| **running**| **waiting**]]

構文の説明

interface	（任意）インターフェイスに現在設定されている NHS 情報を表示します。タイプ、番号範囲、説明については、下の表を参照してください。
detail	（任意）詳細な NHS 情報を表示します。
redundancy	（任意）NHS 冗長スタックに関する情報を表示します。
cluster*number*	（任意）冗長クラスタ情報を表示します。
preempted	（任意）アクティブになれず、プリエンプション処理された NHS に関する情報を表示します。
running	（任意）現在「Responding」または「Expecting replies」状態になっている NHS を表示します。
waiting	（任意）スケジュール処理待ち状態の NHS 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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

次の表に、任意指定の *interface* 引数の有効なタイプ、番号の範囲、および説明を示します。

（注） 有効なタイプは、プラットフォームとプラットフォーム上のインターフェイスによって異なります。

表 *21*：有効なタイプ、番号の範囲、およびインターフェイスの説明

有効なタイプ	番号の範囲	インターフェイスの説明
ANI	0 ～ 1000	自律型ネットワーク仮想インターフェイス
Auto-Template	1 ～ 999	自動テンプレート インターフェイス
Capwap	0 ～ 2,147,483,647	Control and Provisioning of Wireless Access Points プロトコル（CAPWAP）トンネル インターフェイス
GMPLS	0 ～ 1000	マルチプロトコル ラベル スイッチング（MPLS）インターフェイス
GigabitEthernet	0 ～ 9	GigabitEthernet IEEE 802.3z
InternalInterface	0 ～ 9	内部インターフェイス
LISP	0 ～ 65520	Locator/ID Separation Protocol（LISP）仮想インターフェイス
loopback	0 ～ 2,147,483,647	ループバック インターフェイス

有効なタイプ	番号の範囲	インターフェイスの説明
Null	0 ～ 0	ヌル インターフェイス
PROTECTION_GROUP	0 ～ 0	保護グループ コントローラ
Port-channel	1 ～ 128	ポート チャネル インターフェイス
TenGigabitEthernet	0 ～ 9	TenGigabitEthernet インターフェイス
Tunnel	0 ～ 2,147,483,647	トンネル インターフェイス
Tunnel-tp	0 ～ 65535	MPLS トランスポート プロファイル インターフェイス
Vlan	1 ～ 4094	VLAN インターフェイス

次に、**show ip nhrp nhs detail** コマンドの出力例を示します。

```
Switch# show ip nhrp nhs detail

Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
   10.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 10.1.1.1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *22*：*show ip nhrp nhs* のフィールドの説明

フィールド	説明
Tunnel1	ターゲット ネットワークに到達するために経由するインターフェイス。

関連コマンド

コマンド	説明
ipnhrpmap	NBMA ネットワークに接続された IP 宛先の IP-to-NBMA アドレス マッピングをスタティックに設定します。
showipnhrp	NHRP マッピング情報を表示します。

show key chain

キーチェーンを表示するには、**show key chain** コマンドを使用します。

show key chain [*name-of-chain*]

構文の説明

name-of-chain	（任意）キー チェーン コマンドで命名された表示対象のキー チェーン名。

コマンド デフォルト

パラメータを指定せずにコマンドを使用すると、すべてのキー チェーンのリストを表示します。

コマンド モード

特権 EXEC（#）

次に、**showkeychain** コマンドの出力例を示します。

```
show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
    key 1 -- text "Thisisasecretkey"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
    key 100 -- text "abc123"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

関連コマンド

コマンド	説明
key-string	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。

show track

トラッキング プロセスが追跡したオブジェクトに関する情報を表示するには、特権 EXEC モードで **showtrack** コマンドを使用します。

show track [*object-number* **[brief]**| **application [brief]**| **interface [brief]**| **ip[route [brief]** | **[sla [brief]]**| **ipv6 [route [brief]]**| **list [route [brief]]**| **resolution [ip** | **ipv6]**| **stub-object [brief]**| **summary**| **timers**]

構文の説明

object-number	（任意）トラッキング対象オブジェクトを表すオブジェクト番号。範囲は 1 ～ 1000 です。
brief	（任意）先行する引数やキーワードに関連する 1 行の情報を表示します。
application	（任意）トラッキング対象のアプリケーション オブジェクトを表示します。
interface	（任意）トラッキング対象のインターフェイス オブジェクトを表示します。
ip route	（任意）トラッキング対象の IP ルート オブジェクトを表示します。
ip sla	（任意）トラッキング対象の IP SLA オブジェクトを表示します。
ipv6 route	（任意）トラッキング対象の IPv6 ルート オブジェクトを表示します。
list	（任意）ブール オブジェクトを表示します。
resolution	（任意）トラッキング対象パラメータの解像度を表示します。
summary	（任意）指定されたオブジェクトの概要を表示します。
timers	（任意）ポーリング間隔タイマーを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
XE 3.10S	このコマンドが変更されました。出力が拡張され、IPv6 ルート情報が表示されるようになりました。

使用上のガイドライン

トラッキング プロセスによってトラッキングされているオブジェクトに関する情報を表示するには、このコマンドを使用します。引数やキーワードを指定しない場合は、すべてのオブジェクトの情報が表示されます。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できるかどうかは、使用可能なCPUによって異なります。特定のサイトトラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

次に、インターフェイスで IP ルーティングの状態をトラッキングした場合の例を示します。

```
Device# show track 1

Track 1
 Interface GigabitEthernet 1/0/1 ip routing
 IP routing is Down (no IP addr)
  1 change, last change 00:01:08
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *23*：*show track* フィールドの説明

フィールド	説明
Track	トラッキング対象オブジェクトの数。
Interface GigabitEthernet 1/0/1 IP routing	インターフェイスタイプ、インターフェイス番号、およびトラッキング対象オブジェクト。
IP routing is	[アップ（Up）] または [ダウン（Down）] で表示されるオブジェクトの状態の値。オブジェクトがダウンしている場合は、理由が示されます。

フィールド	説明
1 change、last change	トラッキング対象オブジェクトの状態が変更された回数と、最後の変更からの経過時間（hh:mm:ss で表示）。

関連コマンド

コマンド	説明
show track resolution	追跡対象パラメータの解像度を表示します。
trackinterface	インターフェイスをトラッキングされるように設定し、トラッキング コンフィギュレーション モードを開始します。
trackiproute	IP ルートの状態を追跡し、トラッキング コンフィギュレーション モードを開始します。

track

Gateway Load Balancing Protocol（GLBP）の重み付けがインターフェイスの状態に基づいて変更されている場合にトラッキング対象インターフェイスを設定するには、グローバル コンフィギュレーション モードで **track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

track *object-number* **interface** *type number* {**line-protocol**| **ip routing** | **ipv6 routing**}

no track *object-number* **interface** *type number* {**line-protocol**| **ip routing** | **ipv6 routing**}

構文の説明

object-number	トラッキングされるインターフェイスを表すオブジェクト番号。値の範囲は 1 ～ 1000 です。
interface*typenumber*	トラッキングするインターフェイス タイプおよび番号。
line-protocol	インターフェイスがアップ状態かどうかをトラッキングします。

iprouting	インターフェイスがアップの状態であることをGLBP に報告する前に、IP ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。
ipv6routing	インターフェイスがアップの状態であることをGLBP に報告する前に、IPv6 ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。

コマンド デフォルト

インターフェイスの状態はトラッキングされません。

コマンド モード

グローバル コンフィギュレーション（config）

使用上のガイドライン

トラッキング対象インターフェイスのパラメータを設定するには、**track** と併せて **glbpweighting** 及び **glbpweightingtrack** コマンドを使用します。GLBP デバイスのトラッキング対象インターフェイスがダウンすると、そのデバイスの重み値は減らされます。重み値が指定された最小値を下回った場合、デバイスは、アクティブ GLBP 仮想フォワーダとしての機能を失います。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できるかどうかは、使用可能な CPU によって異なります。特定のサイトトラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

次に、TenGigabitEthernet インターフェイス 0/0/1 が、GigabitEthernet インターフェイス 1/0/1 および 1/0/3 がアップの状態にあるかどうかをトラッキングする例を示します。GigabitEthernet インターフェイスのいずれかがダウンすると、GLBP の重み値は、デフォルト値である 10 まで減らされます。両方の GigabitEthernet インターフェイスがダウンすると、GLBP の重み値は下限しきい値未満に下がり、デバイスはアクティブフォワーダではなくなります。アクティブフォワーダとしての役割を再開するには、デバイスは、両方のトラッキング対象インターフェイスをアップの状態に戻し、重み値を上限しきい値を超える値に上げる必要があります。

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
```

```
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2
```

関連コマンド

コマンド	説明
glbpweighting	GLBPゲートウェイの初期重み値を指定します。
glbpweightingtrack	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。

vrrp

Virtual Router Redundancy Protocol バージョン 3（VRRPv3）グループを作成し、VRRPv3 グループコンフィギュレーション モードを開始するには、**vrrp** を使用します。VRRPv3 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。

vrrp *group-id* **address-family** {**ipv4** | **ipv6**}

no vrrp *group-id* **address-family** {**ipv4** | **ipv6**}

構文の説明

group-id	仮想ルータ グループ番号。範囲は 1 ～ 255 です。
address-family	このVRRPグループのアドレスファミリを指定します。
ipv4	（任意）IPv4 アドレスを指定します。
ipv6	（任意）IPv6 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

インターフェイス コンフィギュレーション（config-if）

使用上のガイドライン

次の例は、VRRPv3 グループの作成方法と VRRP コンフィギュレーション モードの開始方法を示しています。

```
Device(config-if)# vrrp 3 address-family ipv4
```

関連コマンド

コマンド	説明
timersadvertise	アドバタイズメントタイマーを設定します（ミリ秒単位）。

vrrp description

Virtual Router Redundancy Protocol（VRRP）に説明を割り当てるには、インターフェイス コンフィギュレーション モードで **vrrpdescription** 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。

description *text*

no description

構文の説明

text	グループの目的または用途を説明するテキスト（最大 80 文字）。

コマンド デフォルト

VRRP グループの説明はありません。

コマンド モード

VRRP 設定（config-if-vrrp）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

次の例では、VRRP を有効にしています。VRRP グループ 1 は、「Building A – Marketing and Administration（ビルディング A：マーケティングおよび管理）」と説明されます。

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループコンフィギュレーションモードを開始します。

vrrp preempt

デバイスに現在のマスター仮想ルータより高い優先順位が与えられている場合、そのデバイスが Virtual Router Redundancy Protocol（VRRP）グループのマスター仮想ルータの機能を引き継ぐように設定するには、VRRP コンフィギュレーション モードで **preempt** 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。

preempt [**delay minimum** *seconds*]

no preempt

構文の説明

delayminimum*seconds*	（任意）マスターの所有権を要求するアドバタイズメントを発行するまでに、デバイスが待機する秒数。デフォルト遅延値は 0 秒です。

コマンド デフォルト

このコマンドは有効です。

コマンド モード

VRRP 設定（config-if-vrrp）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

デフォルトでは、このコマンドで設定されるデバイスは、現在のマスター仮想ルータよりも高い優先順位を持つ場合、マスター仮想ルータとしての機能を引き継ぎます。VRRP デバイスが、マスター所有権を要求するアドバタイズメントを発行するまで、指定された秒数待機するように遅延時間を設定できます。

（注） このコマンドの設定にかかわらず、IP アドレスの所有者であるデバイスがプリエンプション処理します。

次に、デバイスの 200 の優先順位が現在のマスター仮想ルータの優先順位よりも高い場合に、デバイスが現在のマスター仮想ルータをプリエンプション処理するように設定する例を示します。デバイスは、現在のマスター仮想ルータをプリエンプション処理する場合、マスター仮想ルータであることを要求するアドバタイズメントを発行するまでに 15 秒待機します。

```
Device(config-if-vrrp)#preempt delay minimum 15
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループコンフィギュレーションモードを開始します。
priority	VRRP グループ内のデバイスの優先度レベルを設定します。

vrrp priority

Virtual Router Redundancy Protocol（VRRP）内のデバイスの優先度レベルを設定するには、インターフェイス コンフィギュレーション モードで **priority** コマンドを使用します。デバイスの優先度レベルを削除するには、このコマンドの **no** 形式を使用します。

priority *level*

no priority *level*

構文の説明

level	VRRP グループ内のデバイスの優先順位。有効な範囲は 1 ～ 254 です。デフォルトは 100 です。

コマンド デフォルト

優先度レベルはデフォルト値の 100 に設定されています。

コマンド モード

VRRP 設定（config-if-vrrp）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

このコマンドを使用すると、どのデバイスをマスター仮想ルータにするかを制御できます。

次に、デバイスを 254 の優先順位に設定する例を示します。

```
Device(config-if-vrrp)# priority 254
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループコンフィギュレーションモードを開始します。
vrrppreempt	デバイスに現在のマスター仮想ルータより高い優先順位が与えられている場合、そのデバイスが VRRP グループのマスター仮想ルータの機能を引き継ぐように設定します。

vrrp timers advertise

Virtual Router Redundancy Protocol（VRRP）グループ内のマスター仮想ルータによる連続したアドバタイズメント間の間隔を設定するには、VRRP コンフィギュレーションモードで **timersadvertise** 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。

timers advertise [msec] *interval*

no timers advertise [msec] *interval*

構文の説明

group	仮想ルータ グループ番号。グループ番号の範囲は 1 ～ 255 です。
msec	（任意）アドバタイズメント時間の単位を秒からミリ秒に変更します。このキーワードを付加しないと、アドバタイズメント間隔は秒単位になります。
interval	マスター仮想ルータによる連続したアドバタイズメント間の時間間隔。**msec** キーワードを指定しなかった場合、間隔は秒単位になります。デフォルト値は 1 秒です。有効範囲は 1 ～ 255 秒です。**msec** キーワードを指定した場合、有効な範囲は 50 ~ 999 ミリ秒です。

コマンド デフォルト

デフォルトの間隔である 1 秒に設定されています。

コマンド モード

VRRP 設定（config-if-vrrp）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

マスター仮想ルータから送信されるアドバタイズメントは、現在のマスター仮想ルータの状態と優先順位を伝えます。

vrrptimersadvertise コマンドは、連続するアドバタイズメント パケットの間の時間間隔と、マスター ルータがダウンしていると他のルータが宣言するまでの時間を設定します。タイマー値が設定されていないルータまたはアクセス サーバは、マスター ルータからタイマー値を取得できます。マスター ルータで設定されたタイマーは、他のすべてのタイマー設定を常に上書きします。VRRP グループ内のすべてのルータが同じタイマー値を使用する必要があります。同じタイマー値が設定されていないと、VRRP グループ内のデバイスが相互通信せず、正しく設定されていないデバイスのステートがマスターに変わります。

次に、マスター仮想ルータがアドバタイズメントを 4 秒ごとに送信するように設定する例を示します。

```
Device(config-if-vrrp)# timers advertise 4
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
timerslearn	VRRP グループのバックアップ仮想ルータとして動作するときに、マスター仮想ルータが使用していたアドバタイズ間隔を学習するようにデバイスを設定します。

vrrs leader

リーダーの名前を Virtual Router Redundancy Service（VRRS）に登録されるように指定するには、**vrrs leader** コマンドを使用します。指定された VRRS リーダーを削除するには、このコマンドの **no** 形式を使用します。

vrrs leader *vrrs-leader-name*

no vrrs leader *vrrs-leader-name*

構文の説明

vrrs-leader-name	リードする VRRS タグの名前。

コマンド デフォルト

登録済み VRRS 名はデフォルトで使用不可になっています。

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

次に、VRRS に登録されるリーダーの名前を指定する例を示します。

```
Device(config-if-vrrp)# vrrs leader leader-1
```

関連コマンド

コマンド	説明
vrrp	VRRP グループを作成し、VRRP コンフィギュレーション モードを開始します。

第 VI 部

IP マルチキャスト ルーティング コマンド

- IP マルチキャスト コマンド，339 ページ

第 7 章

IP マルチキャスト コマンド

- cache-memory-max, 340 ページ
- clear ip mfib counters, 341 ページ
- clear ip mroute, 343 ページ
- ip igmp filter, 344 ページ
- ip igmp max-groups, 345 ページ
- ip igmp profile, 347 ページ
- ip igmp snooping, 348 ページ
- ip igmp snooping last-member-query-count, 349 ページ
- ip igmp snooping querier, 351 ページ
- ip igmp snooping report-suppression, 353 ページ
- ip igmp snooping vlan mrouter, 354 ページ
- ip igmp snooping vlan static, 356 ページ
- ip multicast auto-enable, 357 ページ
- ip multicast vlan, 358 ページ
- ip pim accept-register, 359 ページ
- ip pim bsr-candidate, 360 ページ
- ip pim rp-candidate, 362 ページ
- ip pim send-rp-announce, 364 ページ
- ip pim spt-threshold, 365 ページ
- match message-type, 366 ページ
- match service-type, 367 ページ

- match service-instance, 368 ページ
- mrinfo, 369 ページ
- redistribute mdns-sd, 370 ページ
- service-list mdns-sd, 371 ページ
- service-policy-query, 373 ページ
- service-routing mdns-sd, 373 ページ
- service-policy, 374 ページ
- show ip igmp filter, 375 ページ
- show ip igmp profile, 376 ページ
- show ip igmp snooping, 377 ページ
- show ip igmp snooping groups, 379 ページ
- show ip igmp snooping igmpv2-tracking, 380 ページ
- show ip igmp snooping mrouter, 381 ページ
- show ip igmp snooping querier, 382 ページ
- show ip igmp snooping wireless mcast-spi-count, 384 ページ
- show ip igmp snooping wireless mgid, 384 ページ
- show ip pim autorp, 386 ページ
- show ip pim bsr-router, 386 ページ
- show ip pim bsr, 387 ページ
- show ip pim tunnel, 388 ページ
- show mdns cache, 390 ページ
- show mdns requests, 391 ページ
- show mdns statistics, 392 ページ
- show platform ip multicast, 393 ページ
- wireless mdns-bridging, 400 ページ
- wireless multicast, 401 ページ

cache-memory-max

キャッシュに使用するシステム メモリの割合を設定するには、**cache-memory-max** コマンドを使用します。キャッシュに使用するシステム メモリの割合を削除するには、このコマンドの **no** 形式を使用します。

cache-memory-max *cache-config-percentage*

no cache-memory-max *cache-config-percentage*

構文の説明

cache-config-percentage	キャッシュに使用するシステム メモリの割合。

コマンド デフォルト

10 %。

コマンド モード

mDNS 設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

ネットワークで学習されるサービスの数が大きくなる可能性があるため、使用できるキャッシュ メモリの容量には上限があります。デフォルトでは、このメモリがシステム メモリの最大10%に設定されています。

（注） デフォルト値は、次のコマンドを使用してオーバーライドできます。

新しいレコードを追加しようとする場合、キャッシュがいっぱいになると、キャッシュ内の期限切れに近いレコードが削除され、新しいレコードのためのスペースが確保されます。

例

次に、キャッシュに使用するシステム メモリの割合を 20 % に設定する例を示します。

```
デバイス(config-mdns)# cache-memory-max 20
```

clear ip mfib counters

すべてのアクティブ IPV4 マルチキャスト転送情報ベース（MFIB）トラフィック カウンタをクリアするには、**clear ip mfib counters** 特権 EXEC コマンドを使用します。

clear ip mfib [**global** | **vrf** *] **counters** [*group-address*] [*hostname* | *source-address*]

構文の説明

global	（任意）IPマルチキャスト転送情報ベース キャッシュをグローバルデフォルト設定にリセットします。
vrf*	（任意）すべての VPN ルーティングおよび転送インスタンスの IP マルチキャスト転送情報ベース キャッシュをクリアします。
group-address	（任意）アクティブ マルチキャスト転送情報ベース（MFIB）トラフィック カウンタを指定されたグループ アドレスに制限します。
hostname | *source-address*	（任意）アクティブ マルチキャスト転送情報ベース（MFIB）トラフィック カウンタを指定されたホスト名または送信元アドレスに制限します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、すべてのマルチキャスト テーブルのアクティブ MFIB トラフィック カウンタをすべてリセットする例を示します。

```
Device# clear ip mfib counters
```

次に、IP マルチキャスト転送情報ベース キャッシュ カウンタをグローバル デフォルト設定にリセットする例を示します。

```
Device# clear ip mfib global counters
```

次に、すべての VPN ルーティングおよび転送インスタンスの IP マルチキャスト転送情報ベースキャッシュをクリアする例を示します。

```
Device# clear ip mfib vrf * counters
```

clear ip mroute

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

clear ip mroute [**vrf** *vrf-name*]{***** | *ip-address* | *group-address*}[*hostname* | *source-address*]

構文の説明

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティング/転送（VRF）インスタンスに割り当てられている名前を指定します。
*****	すべてのマルチキャスト ルートを指定します。
ip-address	IP アドレスのマルチキャスト ルート。
group-address	グループ アドレスのマルチキャスト ルート。
hostname	（任意）ホスト名のマルチキャスト ルート。
source-address	（任意）送信元アドレスのマルチキャスト ルート。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

group-address 変数は、次のいずれかを指定します。

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

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

例

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

```
Device# clear ip mroute *
```

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

```
Device# clear ip mroute 224.2.205.42 228.3.0.0
```

ip igmp filter

Internet Group Management Protocol（IGMP）プロファイルをインターフェイスに適用することで、レイヤ 2 インターフェイスのすべてのホストが 1 つ以上の IP マルチキャスト グループに参加できるかどうかを制御するには、デバイス スタックまたはスランドアロン デバイスで **ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp filter *profile number*

no ip igmp filter

構文の説明

profile number	適用するIGMPプロファイル番号。指定できる範囲は1～4294967295です。

コマンド デフォルト

IGMP 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
Cisco IOS XE 3.2SE	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、Switch Virtual Interface（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 プロファイルは 1 つまたは複数のデバイス 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

次に、IGMPプロファイル40を設定して、指定した範囲のIPマルチキャストアドレスを許可し、その後、プロファイルをフィルタとしてポートに適用する例を示します。

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 233.1.1.1 233.255.255.255
Device(config-igmp-profile)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport
*Jan  3 18:04:17.007: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down.
NOTE: If this message appears, this interface changes to layer 2, so that you can apply the
 filter.
Device(config-if)# ip igmp filter 40
```

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。

ip igmp max-groups

レイヤ 2 インターフェイスが参加可能な Internet Group Management Protocol（IGMP）グループの最大数を設定するか、最大数のエントリが転送テーブルにあるときの IGMP スロットリング アクションを設定するには、デバイス スタックまたはスタンドアロン デバイスで **ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。最大数をデフォルト値（無制限）に戻すか、デフォルトのスロットリング アクション（レポートをドロップ）に戻すには、このコマンドの **no** 形式を使用します。

ip igmp max-groups {*max number* | **action** { **deny** | **replace**}}

no ip igmp max-groups {*max number* | **action**}

構文の説明

max number	インターフェイスが参加できる IGMP グループの最大数。指定できる範囲は 0 ～ 4294967294 です。デフォルト設定は無制限です。
action deny	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は、次の IGMP 参加レポートをドロップします。これがデフォルトのアクションになります。
action replace	最大数のエントリが IGMP スヌーピング転送テーブルにある場合に、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で置き換えます。

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デバイスが学習した後の、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
Cisco IOS XE 3.2SE	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、Switch Virtual Interface（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 レポートをデバイスがドロップします。
- 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、デバイス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レポートで置き換えます。

- 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。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp max-groups 25
```

次に、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デバイスを設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(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。

ip igmp profile

Internet Group Management Protocol（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、デバイス スタックまたはスタンドアロン デバイスで **ip igmp profile** グローバル コンフィギュレーション コマンドを使用します。このモードで、スイッチ ポートからのIGMPメンバーシップ 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。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
Cisco IOS XE 3.2SE	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ように指定します（デフォルト設定の状態）。
- **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にする、またはデフォルトにリセットします。
- **permit**：一致するアドレスを許可するように指定します。
- **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で範囲を指定することもできます。

  範囲を入力する場合、低い方の IP マルチキャスト アドレスを入力してからスペースを入力し、次に高い方の IP マルチキャスト アドレスを入力します。

IGMP のプロファイルを、1 つまたは複数のレイヤ 2 インターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは 1 つだけです。

例

次の例では、IP マルチキャスト アドレスの範囲を指定した IGMP プロファイル 40 の設定方法を示します。

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

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

ip igmp snooping

デバイス で Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングをグローバルにイネーブルにするか、または VLAN 単位でイネーブルにするには、デバイス スタックまたはスタンドアロン デバイスで **ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no ip igmp snooping [**vlan** *vlan-id*]

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。

コマンド デフォルト

デバイス上で、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
Cisco IOS XE 3.2SE	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。

```
Device(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。

```
Device(config)# ip igmp snooping vlan 1
```

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

ip igmp snooping last-member-query-count

Internet Group Management Protocol（IGMP）スヌーピングが IGMP 脱退メッセージの受信に対してクエリー メッセージを送信する回数を設定するには、グローバル コンフィギュレーション モー

ドで **ipigmpsnoopinglast-member-query-count** コマンドを使用します。*count* 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。

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

構文の説明

vlan*vlan-id*	（任意）特定の VLAN ID のカウント値を指定します。範囲は 1 ～ 1001 です。先頭の 0 は入力しないでください。
count	クエリー メッセージの送信インターバルを、ミリ秒単位で設定します。指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。

コマンド デフォルト

クエリーが 2 ミリ秒ごとに送信されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 ホストがグループから脱退すると、ホストは IGMP 脱退メッセージを送信します。このホストがグループを脱退する最終ホストかどうかを確認するために、脱退メッセージが確認されると、**last-member-query-interval** タイムアウト期間が過ぎるまで IGMP クエリー メッセージが送信されます。タイムアウト期限が切れる前に last-member クエリーへの応答が受信されないと、グループ レコードは削除されます。

タイムアウト期間を設定するには、**ip igmp snooping last-member-query-interval** コマンドを使用します。

IGMP スヌーピング即時脱退処理とクエリー カウントの両方を設定した場合は、即時脱退処理が優先されます。

（注） カウントを 1 に設定しないでください。単一パケットの損失（デバイスからホストへのクエリー パケット、またはホストからデバイスへのレポート パケット）により、受信者がいてもトラフィックの転送が停止される場合があります。トラフィックは、次の一般クエリーがデバイスから送信された後も転送され続けますが、受信者がクエリーを受信しない間隔は 1 分間（デフォルトのクエリー間隔で）となる可能性があります。

Cisco IOS ソフトウェアの脱退遅延は、デバイスが last-member-query-interval（LMQI）内で複数の脱退を処理しているときに、1 つの LMQI 値まで増やすことができます。この場合、平均脱退遅延は (カウント数 + 0.5) * LMQI によって決まります。その結果、デフォルトの脱退遅延は 2.0 ～ 3.0 秒の範囲となり、IGMP 脱退処理の負荷が高い状態では平均 2.5 秒となります。100 ミリ秒でカウントが 1 という LMQI の最小値の負荷条件下では、脱退遅延は 100 ～ 200ミリ秒となり、平均は 150 ミリ秒です。これは、高レートの IGMP 脱退メッセージから受ける影響を抑えるために行われます。

次に、最後のメンバ クエリーの数を 5 に設定する例を示します。

```
Device(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

レイヤ 2 ネットワークで Internet Group Management Protocol（IGMP）クエリア機能をグローバルにイネーブルにするには、 **ip igmp snooping querier** グローバル コンフィギュレーション コマンドを使用します。キーワードとともにコマンドを入力すると、VLAN インターフェイスの IGMP クエリア機能をイネーブルにし、設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {**count** *count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*]

no ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** | **max-response-time** | **query-interval** | **tcn query** {**count** | **interval**} | **timer expiry** | **version**]

構文の説明

vlan*vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび IGMP クエリア機能をイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
address*ip-address*	（任意）送信元 IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。
max-response-time*response-time*	（任意）IGMP クエリア レポートを待機する最長時間を設定します。値の範囲は 1 ～ 25 秒です。

query-interval*interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
tcn query	（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。
count*count*	TCN 時間間隔に実行される TCN クエリの数を設定します。指定できる範囲は 1 ～ 10 です。
interval*interval*	TCN クエリの時間間隔を設定します。指定できる範囲は 1 ～ 255 です。
timer expiry *expiry-time*	（任意）IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ～ 300 秒です。
version*version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。

コマンド デフォルト

IGMP スヌーピング クエリア機能は、デバイスでグローバルにディセーブルに設定されています。

IGMP スヌーピング クエリアは、イネーブルの場合でも、マルチキャスト ルータからの IGMP トラフィックが検出されると、自らをディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 メッセージを送信するデバイスの IGMP バージョンおよび IP アドレスを検出するために IGMP スヌーピングをイネーブルにするには、このコマンドを使用します。

デフォルトでは、IGMP スヌーピング クエリアは、IGMP バージョン 2（IGMPv2）を使用するデバイスを検出するよう設定されていますが、IGMP バージョン 1（IGMPv1）を使用しているクライアントは検出しません。デバイスが IGMPv2 を使用している場合、max-response-time 値を手動

で設定できます。デバイスが IGMPv1 を使用している場合は、max-response-time を設定できません（値を設定できず、0 に設定されています）。

IGMPv1 を実行している RFC に準拠していないデバイスは、max-response-time 値としてゼロ以外の値を持つ IGMP 一般クエリ 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 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。

```
Device(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。

```
Device(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。

```
Device(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。

```
Device(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。

```
Device(config)# ip igmp snooping querier timer 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。

```
Device(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。

ip igmp snooping report-suppression

Internet Group Management Protocol（IGMP）レポート抑制をイネーブルにするには、デバイス スタックまたはスタンドアロンデバイスで **ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。IGMP レポート抑制をディセーブルにして、すべての IGMP レポートをマルチキャスト ルータに転送するには、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。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

デバイス 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 クエリごとに 1 つの IGMP レポートのみをマルチキャスト デバイスに転送します。IGMP レポート抑制がイネーブル（デフォルト）である場合、デバイス は最初の IGMP レポートをグループのすべてのホストからすべてのマルチキャスト ルータに送信します。デバイス 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 クエリに IGMPv1 および IGMPv2 レポートに対する要求のみが含まれている場合、デバイス は最初の IGMPv1 レポートまたは IGMPv2 レポートのみを、グループのすべてのホストからすべてのマルチキャスト ルータに転送します。マルチキャスト ルータ クエリに IGMPv3 レポートに対する要求も含まれる場合、デバイス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 ルータに転送されます。

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。

```
Device(config)# no ip igmp snooping report-suppression
```

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

ip igmp snooping vlan mrouter

マルチキャスト ルータ ポートの追加、デバイス スタックまたはスタンドアロン デバイスで、**ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id*}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id*}

構文の説明

vlan-id	IGMP スヌーピングをイネーブルにして、指定した VLAN のポートをマルチキャスト ルータ ポートとして追加します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
interface *interface-id*	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。引数の意味は次のとおりです。 • *gigabitethernet interface number*：ギガビット イーサネット IEEE 802.3z インターフェイス。 • *tengigabitethernet interface number*：10 ギガビット イーサネット IEEE 802.3z インターフェイス。 • *port-channel interface number*：チャネル インターフェイス。指定できる範囲は 0 ～ 128 です。

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、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。

```
Device(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

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

ip igmp snooping vlan static

Internet Group Management Protocol（IGMP）スヌーピングをイネーブルにし、マルチキャスト グループのメンバとしてレイヤ 2 ポートをスタティックに追加するには、デバイス スタックまたはスタンドアロン デバイスで **ip igmp snooping vlan static** グローバル コンフィギュレーション コマンドを使用します。スタティックなマルチキャスト グループのメンバとして指定されたポートを削除するには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

構文の説明

vlan-id	指定した VLAN で IGMP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。
ip-address	指定のグループ IP アドレスを持ったマルチキャスト グループのメンバとして、レイヤ 2 ポートを追加します。
interface *interface-id*	メンバ ポートのインターフェイスを指定します。*interface-id* 値には次のオプションがあります。 • *fastethernet interface number*：ファスト イーサネット IEEE 802.3 インターフェイス • *gigabitethernet interface number*：ギガビット イーサネット IEEE 802.3z インターフェイス • *tengigabitethernet interface number*：10 ギガビット イーサネット IEEE 802.3z インターフェイス。 • *port-channel interface number*：チャネル インターフェイス。指定できる範囲は 0 ～ 128 です。

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
Cisco IOS XE 3.2SE	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。

```
Device(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1
Configuring port gigabitethernet1/0/1 on group 224.2.4.12
```

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

ip multicast auto-enable

IP マルチキャストの認証、認可、アカウンティング（AAA）の有効化をサポートするには、**ipmulticastauto-enable** コマンドを使用します。このコマンドによって、RADIUS サーバから、AAA 属性を使用しているダイヤルアップインターフェイスでのマルチキャストルーティングをダイナミックに有効化できます。AAA の IP マルチキャストを無効にするには、このコマンドの **no** 形式を使用します。

ip multicast auto-enable

no ip multicast auto-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

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

このコマンドは、LAN Base イメージを使用している場合は使用できません。

例

次に、IP マルチキャストの認証、許可、アカウンティング（AAA）を有効にする例を示します。

```
Device(config)# ip multicast auto-enable
```

ip multicast vlan

単一の VLAN に IP マルチキャストを設定するには、グローバル コンフィギュレーション モードで **ipmulticastvlan** コマンドを使用します。WLAN から VLAN を削除するには、このコマンドの **no** 形式を使用します。

ip multicast vlan {*vlan-name*| *vlan-id*}

no ip multicast vlan{*vlan-name*| *vlan-id*}

構文の説明

vlan-name	VLAN 名を指定します。
vlan-id	VLAN ID を指定します。

コマンド デフォルト

ディセーブル

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

次に、vlan_id01 をマルチキャスト VLAN として設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast
Device(config)# wlan test-wlan 1
Device(config-wlan)# ip multicast vlan vlan_id01
```

ip pim accept-register

Protocol Independent Multicast（PIM）登録メッセージをフィルタ処理するように候補ランデブー ポイント（RP）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 pim accept-register** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*}

no ip pim [**vrf** *vrf-name*] **accept-register**

構文の説明

vrf *vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（MVRF）インスタンスに関連付けられている (S, G) トラフィック用の候補 RP で PIM 登録フィルタを設定します。
list *access-list*	許可または拒否する PIM 登録メッセージ内の (S, G) トラフィックを定義する数値または名前として、*access-list* 引数を指定します。有効範囲は 100 ～ 199 で、拡張された範囲は 2000 ～ 2699 です。IP 名前付きアクセス リストも使用できます。

コマンド デフォルト

PIM 登録フィルタ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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

不正な送信元が RP に登録されないようにするには、このコマンドを使用します。不正な送信元が RP に登録メッセージを送信すると、RP はただちに登録停止メッセージを送り返します。

ip pim accept-register コマンドに提供されるアクセスリストは IP 送信元アドレスと IP 宛先アドレスでのみをフィルタ処理します。その他のフィールドのフィルタリング（たとえば、IP プロトコルまたは UDP ポート番号）は無効になっています。これらは、共有ツリーの下方の RP からマルチキャストグループメンバーに不要なトラフィックを転送する場合があります。より複雑なフィルタリングが必要な場合は、代わりに、**ip multicast boundary** コマンドを使用します。

例

次に、SSM グループ範囲（232.0.0.0/8）に送信している送信元アドレス 172.16.10.1 を除き、すべてのグループ範囲に送信しているすべての送信元アドレスの登録パケットを許可する例を示します。これらは拒否されます。候補 RP は最初のホップ ルータまたはスイッチから PIM 登録を受信するため、これらのステートメントはすべての候補 RP に設定する必要があります。

```
Device(config)# ip pim accept-register list ssm-range
Device(config)# ip access-list extended ssm-range
Device(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
Device(config-ext-nacl)# permit ip any any
```

ip pim bsr-candidate

候補 BSR にな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 pim bsr-candidate** コマンドを使用します。候補 BSR としてのスイッチを削除するには、このコマンドの **no** 形式を使用します。

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-id* [*hash-mask-length*] [*priority*]

no ip pim [**vrf** *vrf-name*] **bsr-candidate**

構文の説明

vrf *vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスの候補 BSR になるようにスイッチを設定します。

interface-id	このスイッチを候補にするための、BSR アドレスの派生元であるこのスイッチのインターフェイスの ID。このインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
hash-mask-length	（任意）PIMv2 ハッシュ機能がコールされる前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）。同じシード ハッシュを持つグループはすべて、同じランデブー ポイント（RP）に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。ハッシュ マスク長により、1 つの RP を複数のグループで使用できるようになります。デフォルトのハッシュ マスク長は 0 です。
priority	（任意）BSR（C-BSR）候補のプライオリティ。有効な範囲は 0 ～ 255 です。デフォルトのプライオリティは 0 です。最高のプライオリティ値を持つ C-BSR が優先されます。

コマンド デフォルト

スイッチはそれ自体を候補 BSR として通知するように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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドに指定したインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。

このコマンドは、指定されたインターフェイスのアドレスを BSR アドレスとして示す BSR メッセージをすべての PIM ネイバーに送信するようにスイッチを設定します。

このコマンドは、PIM ドメイン内のすべての部分に良好に接続できるバックボーン スイッチで設定する必要があります。

BSR メカニズムは RFC 2362 で指定されています。候補 RP（C-RP）は、ユニキャスト C-RP アドバタイズメント パケットを BSR にスイッチングします。その後、BSR は、これらのアドバタイズメントを BSR メッセージに集約します。BSR メッセージは、TTL 1 で、ALL-PIM-ROUTERS グループのアドレス 224.0.0.13 に定期的にマルチキャストされます。これらのメッセージのマルチ

キャストは、ホップバイホップRPFフラッディングによって処理されます。事前のIPマルチキャストルーティング設定は必要がありません（AutoRPとは異なる）。また、BSRは、特定のグループ範囲について指定されたRPを事前に選択しません（AutoRPとは異なる）。代わりに、BSRメッセージを受信する各スイッチがBSRメッセージ内の情報に基づいてグループ範囲のRPを選択します。

シスコスイッチはBSRメッセージを常に受け入れ、処理します。この機能を無効にするコマンドはありません。

シスコ スイッチは、次の手順で、どのC-RPがグループで使用されているかを判別します。

- BSR C-RPで通知されるグループ プレフィックスに対して最長一致ルックアップを実行します。
- 最長一致ルックアップによってBSRが学習したC-RPが複数見つかった場合は、優先順位が最低のC-RP（**ip pim rp-candidate** コマンドで設定される）が優先されます。
- 複数のBSRが学習したC-RPで優先順位が同じ場合は、グループのRPを選択するために、BSRハッシュ関数が使用されます。
- 複数のBSRが学習したC-RPがBSRハッシュ関数から派生された同じハッシュ値を返す場合は、最高のIPアドレスのBSR C-RPが優先されます。

例

次に、ハッシュ マスク長0および優先順位192を使用して、ギガビット イーサネット インターフェイス1/0/0のスイッチのIPアドレスがBSR C-RPになるように設定する例を示します。

```
Device(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim rp-candidate

自身をProtocol Independent Multicast（PIM）バージョン2（PIMv2）候補ランデブー ポイント（C-RP）としてBSRにアドバタイズ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 pim rp-candidate** コマンドを使用します。C-RPとしてのこのスイッチを削除するには、このコマンドの **no** 形式を使用します。

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-id* [**group-list** *access-list-number*]

no ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-id* [**group-list** *access-list-number*]

構文の説明

vrf *vrf-name*	（任意）*vrf-name*引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスのPIMv2 C-RPとして自身をBSRにアドバタイズするようにスイッチを設定します。

interface-id	対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスの ID。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
group-list *access-list-number*	（任意）RP アドレスに関連してアドバタイズされるグループ プレフィックスを定義する標準 IP アクセス リスト番号を指定します。

コマンド デフォルト

スイッチは PIMv2 C-RP として自身を BSR に通知するように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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

自身を候補 RP として BSR アドバタイズするために PIMv2 メッセージを送信するようにスイッチを設定するには、このコマンドを使用します。

このコマンドは、PIM ドメイン内のすべての部分に良好に接続できるバックボーン スイッチで設定する必要があります。

interface-id によって指定されたインターフェイスに関連付けられている IP アドレスは C-RP アドレスとしてアドバタイズされます。

このコマンドに指定したインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。

オプションの **group-list** キーワードと *access-list-number* 引数が設定されている場合は、RP アドレスとのアソシエーション時に、標準 IP アクセス リストによって定義されたグループ プレフィックスもアドバタイズされます。

例

次に、自身を C-RP として PIM ドメイン内の BSR にアドバタイズするようにスイッチを設定する例を示します。標準アクセス リスト番号 4 により、ギガビット イーサネット インターフェイス 1/0/1 で識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。

```
Device(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

Auto-RP を使用して、スイッチがランデブー ポイント（RP）として動作するグループを設定するには、グローバル コンフィギュレーション モードで **ip pim send-rp-announce** コマンドを使用します。このスイッチの RP としての設定を解除するには、このコマンドの **no** 形式を使用します。

ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id* **scope** *ttl-value* [**group-list** *access-list-number*] [**interval** *seconds*]

no ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id*

構文の説明

vrf *vrf-name*	（任意）スイッチがランデブー ポイント（RP）として動作するグループを設定するには、*vrf-name* 引数に Auto-RP を使用します。
interface-id	RP アドレスを識別するインターフェイスのインターフェイス ID を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
scope *ttl-value*	Auto-RP アナウンスメントの数を制限するホップでの存続可能時間（TTL）を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。
group-list *access-list-number*	（任意）RP アドレスに関連してアドバタイズされるグループ プレフィックスを定義する標準 IP アクセス リスト番号を指定します。IP 標準アクセス リスト番号を入力します。指定できる範囲は 1 ～ 99 です。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。
interval*seconds*	（任意）RP アナウンスメント間の間隔を秒単位で指定します。RP アナウンスメントの合計保留時間は、間隔値の 3 倍に自動設定されます。デフォルト インターバルは 60 秒です。指定できる範囲は 1 ～ 16383 です。

コマンド デフォルト

Auto-RP 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

RPにするスイッチで次のコマンドを入力します。Auto-RP を使用してグループ/RP マッピングを配信すると、ルータはこのコマンドにより既知のグループ CISCO-RP-ANNOUNCE（224.0.1.39）に Auto-RP アナウンスメント メッセージを送信します。このメッセージは、ルータがアクセス リストで規定される範囲内のグループに対する候補 RP であることを通知します。

例

次に、最大 31 ホップのすべての Protocol Independent Multicast（PIM）対応インターフェイスに RP アナウンスメントを送信するようにスイッチを設定する例を示します。スイッチを RP として識別するために使用される IP アドレスは、120 秒間隔でギガビット イーサネット インターフェイス 1/0/1 に関連付けられる IP アドレスです。

```
Device(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5 interval
 120
```

ip pim spt-threshold

最短パス ツリー（spt）に移行する上限値となるしきい値を指定するには、グローバル コンフィギュレーション モードで **ip pim spt-threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。

ip pim {*kbps* | **infinity**} [**group-list** *access-list*]

no ip pim {*kbps* | **infinity**} [**group-list** *access-list*]

構文の説明

kbps	最短パス ツリー（spt）に移行する上限値となるしきい値を指定します。有効な範囲は 0 ～ 4294967 ですが、0 が唯一有効なエントリです。0 エントリは、常に送信元ツリーに切り替わります。
infinity	指定されたグループのすべての送信元が共有ツリーを使用し、送信元ツリーに切り替わらないように指定します。
group-list *access-list*	（任意）アクセス リスト番号を指定するか、または作成した特定のアクセス リストを名前で指定します。値 0 を指定する場合、または **group-list** *access-list* オプションを使用しない場合、しきい値はすべてのグループに適用されます。

コマンド デフォルト

PIM 最短パス ツリー（spt）に切り替わります。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、アクセス リスト 16 のすべての送信元が共有ツリーを使用するように指定する例を示します。

```
Device(config)# ip pim spt-threshold infinity group-list 16
```

match message-type

サービス リストの照合するメッセージ タイプを設定するには、**match message-type** コマンドを使用します。

match message-type {**announcement| any| query**}

構文の説明

announcement	デバイスのサービス アドバタイズメントまたはアナウンスメントのみを許可します。
any	任意の照合タイプを許可します。
query	ネットワーク内の特定のデバイスに対するクライアントからクエリのみを許可します。

コマンド デフォルト

サービス 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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

異なるシーケンス番号を持つ同じ名前の複数のサービス マップを作成することができ、フィルタの評価順序はシーケンス番号に基づきます。サービス リストは、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。サービス リストの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクション permit または deny が実行されると停止します。リスト全体をスキャンした後のデフォルトのアクションは deny です。

（注） **service-list mdns-sd***service-list-name***query** コマンドを使用している場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。

次に、照合されるアナウンスメント メッセージ タイプを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match message-type announcement
```

match service-type

照合する mDNS サービス タイプ文字列値を設定するには、**match service-type** コマンドを使用します。

match service-type *line*

構文の説明

line	パケット内のサービス タイプを照合するための正規表現。

コマンド デフォルト

なし

コマンド モード

サービス 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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

service-list mdns-sd*service-list-name***query** コマンドを使用している場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。

次に、照合する mDNS サービス タイプ文字列値を設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match service-instance

サービス リストの照合するサービス インスタンスを設定するには、**match service-instance** コマンドを使用します。

match servcie-instance *line*

構文の説明

line	パケット内のサービス インスタンスを照合するための正規表現。

コマンド デフォルト

なし

コマンド モード

サービス 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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

service-list mdns-sd*service-list-name***query** コマンドを使用している場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。

次に、照合するサービス インスタンスを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-instance servInst 1
```

mrinfo

ピアとして動作している隣接するマルチキャストルータまたはマルチレイヤスイッチをクエリするには、ユーザ EXEC モードまたは特権 EXEC モードで **mrinfo** コマンドを使用します。

mrinfo [**vrf** *route-name*] [*hostname* | *address*][*interface-id*]

構文の説明

vrf *route-name*	（任意）VPN ルーティングおよび転送インスタンスを指定します。
hostname | *address*	（任意）クエリするマルチキャストルータまたはマルチレイヤスイッチのドメイン ネーム システム（DNS）名または IP アドレス。省略すると、スイッチは自身をクエリします。
interface-id	（任意）インターフェイス ID を指定します。

コマンド デフォルト

このコマンドはディセーブルです。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

mrinfo コマンドは、マルチキャスト ルータまたはスイッチのピアとして動作している隣接するマルチキャスト ルータまたはスイッチを判別するためのマルチキャスト バックボーン（MBONE）のオリジナルのツールです。シスコ ルータは、Cisco IOS リリース 10.2 以降、mrinfo 要求への応答をサポートしています。

mrinfo コマンドを使用して、マルチキャスト ルータまたはマルチレイヤ スイッチをクエリすることができます。出力フォーマットは、マルチキャスト ルーテッド バージョンのディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）と同じです。（mrouted ソフトウェアは、DVMRP を実装する UNIX ソフトウェアです）。

例

次に、**mrinfo** コマンドの出力例を示します。

```
Device# mrinfo
 vrf 192.0.1.0
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```

（注） フラグの意味は次のとおりです。

- P：プルーニング対応
- M：mtrace 対応
- S：Simple Network Management Protocol（SNMP）対応
- A：自動ランデブー ポイント（Auto-RP）対応

redistribute mdns-sd

サブネット全体にサービスやサービス アナウンスメントを再配布するには、**redistribute mdns-sd** コマンドを使用します。サブネット全体へのサービスやサービス アナウンスメントの再配布を無効にするには、このコマンドの **no** 形式を使用します。

redistribute mdns-sd

no redistribute mdns-sd

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

サブネット全体へのサービスやサービス アナウンスメントの再配布は無効になっています。

コマンド モード

mDNS コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	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サービス アナウンスメントを再配布するには、**redistribute mdns-sd** コマンドを使用します。このコマンドは、1 つのインターフェイスで受信した非要請アナウンスメントを他のすべてのインターフェイスに送信します。発信アナウンスメントはインターフェイスに定義された出力サービス ポリシーに従って、または、インターフェイスごとのサービス ポリシーがない場合はグローバル出力サービス ポリシーに基づいてフィルタ処理されます。

再配布オプションがない場合は、サービス プロバイダーに対してローカルでないレイヤ 3 ドメインでクエリすることで、サービスを検出できます。

例

次に、サブネット全体にサービスやサービス アナウンスメントを再配布する例を示します。

```
デバイス(config-mdns)# redistribute mdns-sd
```

（注） 再配布がグローバルに有効になっている場合は、グローバル コンフィギュレーションがインターフェイス コンフィギュレーションよりも優先順位が高くなります。

service-list mdns-sd

デバイスで mDNS サービス検出サービスリスト モードを開始するには、**service-list mdns-sd** コマンドを使用します。mDNS サービス検出サービスリスト モードを終了するには、このコマンドの **no** 形式を使用します。

service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

no service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

構文の説明

service-list-name	サービス リストの名前。
permit *sequence number*	シーケンス番号に対するサービス リストのフィルタの適用を許可します。

deny *sequence number*	シーケンス番号に対するサービス リストのフィルタの適用を拒否します。
query	サービス リスト名のクエリを関連付けます。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	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 フィルタは、アクセス リストとルートマップに関してモデル化されています。

異なるシーケンス番号を持つ同じ名前の複数のサービス マップを作成することができ、フィルタの評価順序はシーケンス番号に基づきます。サービス リストは、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。サービス リストの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクション permit または deny が実行されると停止します。リスト全体をスキャンした後のデフォルトのアクションは deny です。

このコマンドは mDNS サービス検出サービスリスト モードを開始するために使用できます。

このモードでは、次の操作を実行できます。

- サービス リストを作成し、シーケンス番号に適用された **permit** または **deny** オプションに従って、サービス リストにフィルタを適用します。

例

次に、サービス リストを作成し、シーケンス番号に適用された **permit** または **deny** オプションに従って、サービス リストにフィルタを適用する例を示します。

```
デバイス(config)# service-list mdns-sd sl1 permit 3
```

service-policy-query

サービス リストのクエリの周期を設定するには、**service-policy-query** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

service-policy-query [*service-list-query-name service-list-query-periodicity*]

no service-policy-query

構文の説明

service-list-query-name *service-list-query-periodicity*	（任意）サービス リストのクエリの周期を設定します。

コマンド デフォルト

ディセーブル

コマンド モード

mDNS コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

非要請アナウンスメントを送信しないデバイスがあるため、サービスを強制的に学習させ、それらをキャッシュ内で最新に維持するために、このコマンドには、アクティブ クエリ リストに一覧されているサービスが確実にクエリされるようにするアクティブ クエリ機能が含まれています。

例

次に、サービス リストのクエリの周期を設定する例を示します。

```
デバイス(config-mdns)# service-policy-query sl-query1 100
```

service-routing mdns-sd

デバイスの mDNS ゲートウェイ機能を有効にし、マルチキャスト DNS コンフィギュレーション モードを開始するには、**service-routing mdns-sd** コマンドを使用します。デフォルト設定を復元

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** 形式を入力します。

service-routing mdns-sd

no service-routing mdns-sd

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

mDNS ゲートウェイ機能は、インターフェイス単位ではなく、グローバルでのみ有効または無効にすることができます。サービス フィルタ ポリシーと再配布は、グローバルでも、インターフェイス単位でも設定できます。インターフェイス固有の設定は、グローバルな設定より優先されます。

例

次に、デバイスの mDNS ゲートウェイ機能を有効にして、マルチキャスト DNS コンフィギュレーション モードを開始する例を示します。

```
デバイス(config)# service-routing mdns-sd
```

service-policy

サービス リストの着信または発信サービス検出情報にフィルタを適用するには、**service-policy** コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

service-policy *service-policy-name* {**IN** | **OUT**}

no service-policy *service-policy-name* {**IN** | **OUT**}

構文の説明

service-policy-name **IN**	着信サービス検出情報にフィルタを適用します。

service-policy-name **OUT**	発信サービス検出情報にフィルタを適用します。

コマンド デフォルト

ディセーブル

コマンド モード

mDNS コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

デバイスは mDNS パケットをインターセプトします。それらがワイヤレス クライアント宛ての mDNS メッセージ（たとえば、宛先 MAC がクライアントの MAC アドレス）であり、クライアントのモビリティ状態がローカルまたは外部のいずれかの場合、宛先 MAC アドレスはクライアントの MAC アドレスで上書きされ、パケットは関連付けられた CAPWAP トンネルに送信されるようにキューに入れられます。

例

次に、サービスリストの着信サービス検出情報にフィルタを適用する例を示します。

```
デバイス(config-mdns)#  service-policy serv-pol1 IN
```

show ip igmp filter

Internet Group Management Protocol（IGMP）フィルタ情報を表示するには、特権 EXEC コマンドモードで **show ip igmp filter** コマンドを使用します。

show ip igmp [**vrf** *vrf-name*] **filter**

構文の説明

vrf*vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスをサポートします。

コマンド デフォルト

特権 EXEC

IGMP フィルタはデフォルトで有効になっています。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 igmp filter コマンドは、デバイスに定義されているすべてのフィルタに関する情報を表示します。

例

次に、**show ip igmp filter** コマンドの出力例を示します。

```
Device# show ip igmp filter
IGMP filter enabled
```

show ip igmp profile

設定済みのすべての Internet Group Management Protocol（IGMP）プロファイルまたは指定された IGMP プロファイルを表示するには、**show ip igmp profile** 特権 EXEC コマンドを使用します。

show ip igmp [**vrf** *vrf-name*] **profile** [*profile number*]

構文の説明

vrf*vrf-name*	（任意）マルチキャストVPNルーティングおよび転送（VRF）インスタンスをサポートします。
profile number	（任意）表示する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。プロファイル番号が入力されていない場合、すべての IGMP プロファイルが表示されます。

コマンド デフォルト

IGMP プロファイルはデフォルトで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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、デバイスのプロファイル番号 40 に対する **show ip igmp profile** 特権 EXEC コマンドの出力例を示します。

```
Device# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255
```

次に、デバイスに設定されているすべてのプロファイルに対する **show ip igmp profile** 特権 EXEC コマンドの出力例を示します。

```
Device# 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
```

show ip igmp snooping

デバイスまたは VLAN の Internet Group Management Protocol（IGMP）スヌーピング構成を表示するには、ユーザまたは特権 EXEC コマンド モードで **show ip igmp snooping** コマンドを使用します。

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

構文の説明

groups	（任意）IGMP スヌーピング マルチキャスト テーブルを表示します。
mrouter	（任意）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。
querier	（任意）IGMP クエリアの設定情報と動作情報を表示します。
vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。

detail	（任意）動作状態の情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

文字列では、大文字と小文字が区別されます。たとえば、| exclude output と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次の例では、**show ip igmp snooping vlan 1** コマンドの出力を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Device# 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
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
```

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、デバイス上の VLAN すべてのスヌーピング特性を表示します。

```
Device# 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
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
Vlan 2:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
<output truncated>
```

show ip igmp snooping groups

デバイスまたはマルチキャスト情報の Internet Group Management Protocol（IGMP）スヌーピング マルチキャスト テーブルを表示するには、**show ip igmp snooping groups** 特権 EXEC コマンドを使用します。

show ip igmp snooping groups [**vlan** *vlan-id*] [[**count**] | *ip_address*]

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。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、このオプションを使用します。
count	（任意）実エントリの代わりに、指定のコマンド オプションのエントリ総数を表示します。
ip_address	（任意）指定グループ IP アドレスのマルチキャスト グループの特性を表示します。

コマンド モード

特権 EXEC

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、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。デバイスのマルチキャスト テーブルが表示されます。

```
Device# show ip igmp snooping groups
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4       igmp                    Gi1/0/11
1         224.1.4.5       igmp                    Gi1/0/11
2         224.0.1.40      igmp        v2          Gi1/0/15
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3       igmp        v2          Gi2/0/1, Gi2/0/2
```

次の例では、**show ip igmp snooping groups count** コマンドの出力を示します。デバイス上のマルチキャスト グループの総数が表示されます。

```
Device# show ip igmp snooping groups count
Total number of multicast groups: 2
```

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。

```
Device# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi1/0/15
```

show ip igmp snooping igmpv2-tracking

グループおよびIP アドレス エントリを表示するには、特権 EXEC モードで **show ip igmp snooping igmpv2-tracking** コマンドを使用します。

（注） このコマンドでは、有線結合ではなく、ワイヤレス マルチキャストIGMP結合に関するグループおよびIP アドレス エントリのみ表示されます。また、このコマンドでは、ワイヤレス マルチキャストが有効になっている場合のみ出力が表示されます。

構文の説明デフォルト

show ip igmp snooping igmpv2-tracking
特権 EXEC モードには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

show ip igmp snooping mrouter

デバイスまたは指定されたマルチキャスト VLAN の Internet Group Management Protocol（IGMP）スヌーピングの動的に学習され、手動で設定されたマルチキャスト ルータ ポートを表示するには、**show ip igmp snooping mrouter** 特権 EXEC コマンドを使用します。

show ip igmp snooping mrouter [**vlan** *vlan-id*]

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。

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
Cisco IOS XE 3.2SE	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。

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。

文字列では、大文字と小文字が区別されます。たとえば、| exclude output と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次の例では、**show ip igmp snooping mrouter** コマンドの出力を示します。デバイスのマルチキャスト ルータ ポートを表示する方法を示します。

```
Device# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

show ip igmp snooping querier

デバイス に設定されている IGMP クエリアの設定情報と動作情報を表示するには、**show ip igmp snooping querier** ユーザ EXEC コマンドを使用します。

show ip igmp snooping querier [**vlan** *vlan-id*] [**detail**]

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
detail	（任意）IGMP クエリアの詳細情報を表示します。

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
Cisco IOS XE 3.2SE	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 クエリ メッセージを送信する検出デバイス（クエリアとも呼ばれます）の IGMP バージョンと 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 デバイス を指定できます。

show ip igmp snooping querier コマンドの出力にも、クエリアが検出された VLAN およびインターフェイスが表示されます。クエリアが デバイス の場合、出力の Port フィールドには「Router」と

表示されます。クエリアがルータの場合、出力の Port フィールドにはクエリアを学習したポート番号が表示されます。

show ip igmp snooping querier detail ユーザ EXEC コマンドは、**show ip igmp snooping querier** コマンドに類似しています。ただし、**show ip igmp snooping querier** コマンドでは、デバイス クエリアによって最後に検出されたデバイスの IP アドレスのみが表示されます。

show ip igmp snooping querier detail コマンドでは、デバイス 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、次の追加情報が表示されます。

- VLAN で選択されている IGMP クエリア
- VLAN で設定された デバイス クエリア（存在する場合）に関連する設定情報と動作情報

文字列では、大文字と小文字が区別されます。たとえば、| exclude output と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次の例では、**show ip igmp snooping querier** コマンドの出力を示します。

```
Device> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
---------------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

次の例では、**show ip igmp snooping querier detail** コマンドの出力を示します。

```
Device> show ip igmp snooping querier detail
Vlan      IP Address     IGMP Version   Port
-----------------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1
Global IGMP デバイス 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 デバイス querier status
-----------------------------------------------------------
elected querier is 1.1.1.1         on port Fa8/0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

show ip igmp snooping wireless mcast-spi-count

デバイスに送信されるマルチキャスト グループ ID（MGID）ごとのマルチキャスト ステートフル パケット インスペクション（SPI）の数の統計を表示するには、特権 EXEC モードで **show ip igmp snooping wireless mcast-spi-count** コマンドを使用します。

show ip igmp snooping wireless mcast-spi-count

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、**show ip igmp snooping wireless mcast-spi-count** コマンドの出力例を示します。

```
デバイス# show ip igmp snooping wireless mcast-spi-count
Stats for Mcast Client Add/Delete SPI Messages Sent to WCM
MGID    ADD MSGs        Del MSGs
--------------------------------
4160    1323            667
```

show ip igmp snooping wireless mgid

マルチキャスト グループ ID（MGID）マッピングを表示するには、特権 EXEC モードで **show ip igmp snooping wireless mgid** コマンドを使用します。

show ip igmp snooping wireless mgid

構文の説明

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、**show ip igmp snooping wireless mgid** コマンドの出力例を示します。

```
Device# show ip igmp snooping wireless mgid

Total number of L2-MGIDs    = 0

Total number of MCAST MGIDs = 0

 Wireless multicast is Enabled in the system
 Vlan     bcast   nonip-mcast   mcast    mgid    Stdby Flags
 1     Disabled   Disabled   Enabled    Disabled  0:0:1:0
 25    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 34    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 200   Disabled   Disabled   Enabled    Disabled  0:0:1:0
 1002  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1003  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1004  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1005  Enabled    Enabled    Enabled    Disabled  0:0:1:0

Index  MGID                  (S, G, V)
-----------------------------------------------------------
```

show ip pim autorp

Auto-RP に関するグローバル情報を表示するには、特権 EXEC モードで **show ip pim autorp** コマンドを使用します。

show ip pim autorp

構文の説明

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-RP はデフォルトで有効になっています。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、Auto-RP が有効になっているか、無効になっているかを表示します。

例

次に、Auto-RP が有効になっている場合のコマンドの出力例を示します。

```
Device# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

show ip pim bsr-router

PIM（Protocol Independent Multicast）ブートストラップルータ（BSR）プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim bsr-router** コマンドを使用します。

show ip pim bsr-router

構文の説明

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

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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-RP に加えて、BSR RP メソッドを設定できます。BSR RP メソッドを設定すると、このコマンドで BSR ルータの情報が表示されます。

次に、**show ip pim bsr-router** コマンドの出力例を示します。

```
Device# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim bsr

PIM（Protocol Independent Multicast）ブートストラップ ルータ（BSR）プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim bsr** コマンドを使用します。

show ip pim bsr

構文の説明

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

ユーザ EXEC

特権 EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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-RP に加えて、BSR RP メソッドを設定できます。BSR RP メソッドを設定すると、このコマンドで BSR ルータの情報が表示されます。

次に、**show ip pim bsr** コマンドの出力例を示します。

```
Device# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim tunnel

インターフェイス上の PIM（Protocol Independent Multicast）レジスタのカプセル化およびカプセル化解除トンネルに関する情報をするには、**show ip pim tunnel**コマンドを使用します。

show ip pim [**vrf** *vrf-name*] **tunnel** [**Tunnel** *interface-number* | **verbose**]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
Tunnel *interface-number*	（任意）トンネル インターフェイス番号を指定します。
verbose	（任意）MAC カプセル化ヘッダーおよびプラットフォーム固有情報などの追加情報を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

PIM トンネル インターフェイスに関する情報を表示するには、**show ip pim tunnel** を使用します。

PIM トンネル インターフェイスは、PIM スパース モード（PIM-SM）登録プロセスの IPv4 マルチキャスト転送情報ベース（MFIB）で使用されます。IPv4 MFIB では、2 種類の PIM トンネル インターフェイスが使用されます。

- PIM カプセル化トンネル（PIM Encap トンネル）
- PIM カプセル化解除トンネル（PIM Decap トンネル）

PIM Encap トンネルは、（Auto-RP、ブートストラップ ルータ（BSR）、またはスタティック RP の設定を介して）グループからランデブー ポイント（RP）へのマッピングを学習するたびに動的に作成されます。PIM Encap トンネルは、送信元が直接接続されているファーストホップ代表ルータ（DR）から送信されるマルチキャスト パケットをカプセル化するために使用されます。

PIM Encap トンネルと同様、PIM Decap トンネル インターフェイスは動的に作成されますが、グループから RP へのマッピングを学習するたびに RP 上でのみ作成されます。PIM Decap トンネル インターフェイスは、PIM レジスタのカプセル化解除メッセージのために RP によって使用されます。

（注） PIM トンネルは実行コンフィギュレーションには表示されません。

PIM トンネル インターフェイスが作成されると、次の syslog メッセージが表示されます。

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,
changed state to up
```

次に、RP から取得した **show ip pim tunnel** の出力例を示します。この出力は、RP 上の PIM Encap および Decap トンネルを確認するために使用されます。

```
Device# show ip pim tunnel

Tunnel0
   Type  : PIM Encap
  RP    : 70.70.70.1*
  Source: 70.70.70.1
Tunnel1*
  Type  : PIM Decap
  RP    : 70.70.70.1*
  Source: -R2#
```

（注） アスタリスク（*）は、そのルータが RP であることを示します。RP には、PIM Encap トンネルインターフェイスおよびPIM Decap トンネルインターフェイスが常にあるとは限りません。

show mdns cache

デバイスの mDNS キャッシュ情報を表示するには、**show mdns cache** 特権 EXEC コマンドを使用します。

show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*] | **type** *record-type*]

構文の説明

interface *type-number*	（任意）mDNS キャッシュ情報を表示する特定のインターフェイスのタイプと番号を指定します。
name *record-name*	（任意）mDNS キャッシュ情報を表示する特定の名前を指定します。
type *record-type*	（任意）mDNS キャッシュ情報を表示する特定のタイプを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	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

次に、キーワードを指定しない **show mdns cache** コマンドの出力例を示します。

```
デバイス# show mdns cache

==========================================================================================
[<NAME>]                          [<TYPE>][<CLASS>][<TTL>/Remaining][Accessed][If-name][Mac
 Address][<RR Record Data>]

_airplay._tcp.local                   PTR     IN      4500/4455         0        Vl1121
b878.2e33.c7c5 CAMPUS APPLE TV1._airplay._tcp.local

CAMPUS APPLE TV1._airplay._tcp.local SRV     IN      120/75            2        Vl1121
b878.2e33.c7c5 CAMPUS-APPLE-TV1.local

CAMPUS-APPLE-TV1.local                A       IN      120/75            2        Vl1121
b878.2e33.c7c5  121.1.0.254

CAMPUS APPLE TV1._airplay._tcp.local TXT     IN      4500/4455         2        Vl1121
b878.2e33.c7c5  (162) 'deviceid=B8:78:2E:33:C7:C6'

              'features=0x5a7ffff7''flags=0x4'

              'model=AppleT~'~

_ipp._tcp.local                       PTR     IN      4500/4465         2        Vl2
2894.0fed.447f  EPSON XP-400 Series._ipp._tcp.local

EPSON XP-400 Series._ipp._tcp.local  SRV     IN      120/85            2        Vl2
2894.0fed.447f  EPSONC053AA.local

EPSONC053AA.local                     A       IN      120/85            2        Vl2
2894.0fed.447f  121.1.0.251

EPSON XP-400 Series._ipp._tcp.local  TXT     IN      4500/4465         2        Vl2
2894.0fed.447f  (384)'txtvers=1' N XP-400 Series'

              'usbFG=EPSON''usb_MDL=XP~'~

_smb._tcp.local                       PTR     IN      4500/4465         2        Vl2
2894.0fed.447f  EPSON XP-400 Series._smb._tcp.local

EPSON XP-400 Series._smb._tcp.local  SRV     IN      120/85            2        Vl2
2894.0fed.447f  EPSONC053AA.local

EPSON XP-400 Series._smb._tcp.local  TXT     IN      4500/4465         2        Vl2
2894.0fed.447f  (1)'' R2-Access1#
```

show mdns requests

デバイスのレコード名とレコード タイプ情報を含む、未処理の mDNS 要求の情報を表示するには、**show mdns requests** 特権 EXEC コマンドを使用します。

show mdns requests [**detail** | **name** *record-name* | **type** *record-type* [**name** *record-name*]]

構文の説明

detail	詳細な mDNS 要求の情報を表示します。
name *record-name*	名前に基づいた詳細な mDNS 要求の情報を表示します。

type *record-type*	タイプに基づいた詳細な mDNS 要求の情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	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

次に、キーワードを指定しない **show mdns requests** コマンドの出力例を示します。

```
デバイス# show mdns requests
MDNS Outstanding Requests
==================================================
Request name  :   _airplay._tcp.local
Request type  :   PTR
Request class :   IN
--------------------------------------------------
Request name  :   *.*
Request type  :   PTR
Request class :   IN
```

show mdns statistics

デバイスの mDNS の統計情報を表示するには、**show mdns statistics** 特権 EXEC コマンドを使用します。

show mdns statistics {**all** | **service-list** *list-name* | **service-policy** {**all** | **interface** *type-number* }}

構文の説明

all	サービスポリシー、サービスリスト、インターフェイス情報を表示します。
service-list *list-name*	サービス リスト情報を表示します。
service-policy	サービス ポリシー情報を表示します。
interface *type number*	インターフェイス情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	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

次に、**show mdns statistics all** コマンドの出力例を示します。

```
デバイス# show mdns statistics all
 mDNS Statistics
 mDNS packets sent       : 0
 mDNS packets received   : 0
 mDNS packets dropped    : 0
 mDNS cache memory in use: 64224(bytes)
```

show platform ip multicast

プラットフォーム依存 IP マルチキャスト テーブルおよびその他の情報を表示するには、**show platform ip multicast** 特権 EXEC コマンドを使用します。

show platform ip multicast {**groups** | **hardware [detail]** | **interfaces** | **retry**}

構文の説明

groups	グループごとの IP マルチキャスト ルートを表示します。
hardware [**detail**]	ハードウェアにロードされた IP マルチキャスト ルートを表示します。任意指定の **detail** キーワードは、宛先インデックスおよびルート インデックスのポート メンバを表示するために使用します。
interfaces	IP マルチキャスト インターフェイスを表示します。
retry	リトライ キューの IP マルチキャスト ルートを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

次に、グループごとのプラットフォーム IP マルチキャスト ルートを表示する例を示します。

```
Device# show platform ip multicast groups

Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
Token: 0x0000001f6  flags:  C
No RPF interface.
Number of OIF: 0
Flags: 0x10   Pkts : 0
OIF Details:No OIF interface.

DI details
----------
Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f6  index1:0x51f6

Cookie length 56
```

```
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x4 0xe0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
---------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
---------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

==============================================================

RI details
----------

SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f6
RM:fd_const lbl = 0x0
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x0
RM:remote data = 0x1
```

```
============================================================

HTM details
-----------
Handle:0x5d604490 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x5d604518  handle1:0x5d604580


Detailed Resource Information (ASIC# 0)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x5d604518)

KEY - grp_addr:224.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:240.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 4095 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 164
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x5d604580)

KEY - grp_addr:224.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:240.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 4095 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 164
capwap_mgid_present: 0 mgid 0

============================================================


MROUTE ENTRY vrf 0 (*, 224.0.1.40)
Token: 0x0000001f8  flags:  C IC
RPF interface: Vl121(74238750229529173)): SVI
Token:0x00000021  flags: F IC NS
Number of OIF: 1
Flags: 0x10   Pkts : 0
OIF Details:
     Vl121      F IC NS
DI details
----------
Handle:0x603d0000 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f7  index1:0x51f7

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x20 0xe0 0x0 0x1 0x28 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
---------------------------------------

al_rsc_di
RM:index = 0x51f7
RM:pmap = 0x0
RM:cmi = 0x33f
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
```

```
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f7
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
---------------------------------------

al_rsc_di
RM:index = 0x51f7
RM:pmap = 0x0
RM:cmi = 0x33f
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f7
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

================================================================

RI details
----------

SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f7
RM:fd const lbl = 0x8
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x1
RM:remote data = 0x1

================================================================

HTM details
-----------
Handle:0x603d0440 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x603cfae0  sm handle 0:0x603d0590  handle1:0x603d0520
sm handle 1:0x603d1770


Detailed Resource Information (ASIC# 0)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x603cfae0)
```

```
KEY - grp_addr:224.0.1.40 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 6 station_index: 165
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x603d0520)

KEY - grp_addr:224.0.1.40 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 6 station_index: 165
capwap_mgid_present: 0 mgid 0

============================================================


MROUTE ENTRY vrf 0 (*, 239.255.255.250)
Token: 0x0000003b7d  flags:  C
No RPF interface.
Number of OIF: 1
Flags: 0x10   Pkts : 95
OIF Details:
     Vl131      F NS
DI details
----------
Handle:0x606ffba0 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f8  index1:0x51f8

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x20 0xef 0xff 0xff 0xfa 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
---------------------------------------

al_rsc_di
RM:index = 0x51f8
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f8
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
---------------------------------------

al_rsc_di
RM:index = 0x51f8
```

```
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x1
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f8
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

==============================================================

RI details
----------

ASIC# 0
Replication list :
------------------

Total #ri : 0
start_ri : 15
common_ret : 0


ASIC# 1
Replication list :
------------------

Total #ri : 6
start_ri : 15
common_ret : 0

Replication entry rep_ri 0xF #elem = 1
0) ri[0]=50 port=58 dirty=0


ASIC# 2
Replication list :
------------------

Total #ri : 0
start_ri : 0
common_ret : 0


SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f8
RM:fd const lbl = 0x8
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x0
RM:remote data = 0x1

==============================================================

HTM details
```

```
-----------
Handle:0x606ff6f8 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x606ff3e0  sm handle 0:0x60ab9160  handle1:0x606ff378
sm handle 1:0x60ab6cc0


Detailed Resource Information (ASIC# 0)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x606ff3e0)

KEY - grp_addr:239.255.255.250 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 178
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
---------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x606ff378)

KEY - grp_addr:239.255.255.250 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 178
capwap_mgid_present: 0 mgid 0

============================================================
```

wireless mdns-bridging

イーサネット mDNS のサポートを有効にするには、**wireless mdns-bridging** コマンドを使用します。イーサネット mDNS のサポートを無効にするには、このコマンドの **no** 形式を使用します。

wireless mdns-bridging

no wireless mdns-bridging

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

イーサネット mDNS のサポートはデフォルトで有効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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

ワイヤレス マルチキャストが有効な場合にのみ、このコマンドを使用します。

次に、イーサネット mDNS サポートを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast
Device(config)# wireless mdns-bridging
```

wireless multicast

イーサネット マルチキャスト サポートを有効にするには、**wirelessmulticast** コマンドを使用します。

wireless multicast [**non-ip** [**vlan** *vlan-id*]]

構文の説明

non-ip	（任意）マルチキャスト非 IP サポートを設定します。
vlan*vlan-id*	（任意）VLAN にマルチキャスト非 IP を指定します。インターフェイス番号の範囲は 1 ～ 4095 です。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、マルチキャスト非 IP VLAN を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast non-ip vlan 20
```

第 VII 部

IPv6

- IPv6 コマンド，405 ページ

第 8 章

IPv6 コマンド

- ipv6 flow monitor, 405 ページ
- ipv6 traffic-filter, 406 ページ
- show wireless ipv6 statistics , 407 ページ

ipv6 flow monitor

このコマンドは、着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。

以前に作成したフローモニタをアクティブにするには、**ipv6flowmonitor** コマンドを使用します。フロー モニタを非アクティブにするには、このコマンドの **no** 形式を使用します。

ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**| **output**}

no ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**| **output**}

構文の説明

ipv6-monitor-name	着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。
sampler*ipv6-sampler-name*	フロー モニタ サンプラーを適用します。
input	入力トラフィックにフロー モニタを適用します。
output	出力トラフィックにフロー モニタを適用します。

コマンド デフォルト

IPv6 フロー モニタはインターフェイスに割り当てられるまでアクティブになりません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 チャネル インターフェイスには NetFlow モニタを接続できません。両方のサービス モジュール インターフェイスが EtherChannel の一部である場合、両方の物理インターフェイスにモニタを接続する必要があります。

次に、フロー モニタをインターフェイスに適用する例を示します。

```
Device(config)# interface gigabitethernet 1/1/2
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-2 output
Device(config-if)# end
```

ipv6 traffic-filter

このコマンドは、IPv6 トラフィック フィルタを有効にします。

インターフェイスでの IPv6 トラフィックのフィルタリングを有効にするには、**ipv6traffic-filter** コマンドを使用します。インターフェイスでの IPv6 トラフィックのフィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

インターフェイス上で IPv6 トラフィックをフィルタ処理するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。フィルタリングできるトラフィックのタイプと方向は、スイッチ スタックで稼働するフィーチャ セットによって異なります。インターフェイスでの IPv6 トラフィックのフィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 traffic-filter [web] *acl-name*

no ipv6 traffic-filter [web]

構文の説明

web	（任意）WLAN Web ACL の IPv6 アクセス名を指定します。
acl-name	IPv6 アクセス名を指定します。

コマンド デフォルト

インターフェイス上での IPv6 トラフィックのフィルタリングは設定されません。

コマンド モード

wlan

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

物理インターフェイス（レイヤ 2 またはレイヤ 3 ポート）、レイヤ 3 ポート チャネル、またはスイッチ仮想インターフェイス（SVI）で **ipv6 traffic-filter** コマンドを使用できます。

ACL をレイヤ 3 インターフェイス（ポート ACL）の発信または着信トラフィックに、またはレイヤ 2 インターフェイス（ルータ ACL）の着信トラフィックに適用できます。

いずれかのポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタ処理し、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

次に、インターフェイスで IPv6 トラフィックをフィルタ処理する例を示します。

```
Device(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

show wireless ipv6 statistics

このコマンドは、IPv6 パケット カウンタの統計を表示するために使用します。

IPv6 パケット カウンタの統計を表示するには、**show wireless ipv6 statistics** コマンドを使用します。

show wireless ipv6 statistics

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、IPv6 パケット カウンタの統計の概要を表示する例を示します。

```
Device# show wireless ipv6 statistics
NS Forwarding to wireless clients               : Enabled

RS count                                        : 0
RA count                                        : 0
NS count                                        : 0
NA count                                        : 0
Other NDP packet count                          : 0
-----------------------------------------------------
Non-IPv6 packets count                          : 0
Non-IPv6 Multicast Destination MAC packet count : 0
Invalid length packets count                    : 0
Null packets count                              : 0
Invalid Source MAC packets count                : 0
-----------------------------------------------------
TCP packets count                               : 0
UDP packets count                               : 0
Fragmented packets count                        : 0
No next header packets count                    : 0
Other type packets count                        : 0
-----------------------------------------------------
Total packets count                             : 0
-----------------------------------------------------
Blocked RA packets count                        : 0
Blocked NS packets count                        : 0
```

第 VIII 部

レイヤ 2/3

- レイヤ 2/3 コマンド，411 ページ

第 9 章

レイヤ 2/3 コマンド

- channel-group, 412 ページ
- channel-protocol, 416 ページ
- clear lacp, 418 ページ
- clear pagp, 419 ページ
- clear spanning-tree counters, 420 ページ
- clear spanning-tree detected-protocols, 421 ページ
- debug etherchannel, 422 ページ
- debug lacp, 424 ページ
- debug pagp, 425 ページ
- debug platform pm, 426 ページ
- debug platform udld, 428 ページ
- debug spanning-tree , 429 ページ
- interface port-channel, 431 ページ
- lacp max-bundle, 432 ページ
- lacp port-priority, 434 ページ
- lacp rate, 435 ページ
- lacp system-priority, 436 ページ
- pagp learn-method, 437 ページ
- pagp port-priority, 439 ページ
- port-channel, 440 ページ
- port-channel auto, 441 ページ

- port-channel load-balance, 442 ページ
- port-channel load-balance extended, 444 ページ
- port-channel min-links, 445 ページ
- rep admin vlan, 446 ページ
- rep block port, 447 ページ
- rep lsl-age-timer, 449 ページ
- rep lsl-retries, 450 ページ
- rep preempt delay, 450 ページ
- rep preempt segment, 452 ページ
- rep segment, 453 ページ
- rep stcn, 455 ページ
- show etherchannel, 456 ページ
- show interfaces rep detail, 459 ページ
- show lacp, 460 ページ
- show pagp, 464 ページ
- show platform etherchannel, 466 ページ
- show platform pm, 467 ページ
- show rep topology, 468 ページ
- show udld, 470 ページ
- switchport, 474 ページ
- switchport access vlan, 475 ページ
- switchport mode, 477 ページ
- switchport nonegotiate, 480 ページ
- switchport voice vlan, 481 ページ
- udld, 484 ページ
- udld port, 486 ページ
- udld reset, 488 ページ

channel-group

EtherChannel グループにイーサネット ポートを割り当てたり、EtherChannel モードをイネーブルにしたり、この両方を行うには、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。EtherChannel グループからイーサネット 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。

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

no channel-group

構文の説明

auto	個々のポートインターフェイスの auto-LAG 機能をイネーブルにします。 デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
channel-group-number	チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
mode	EtherChannel モードを指定します。
active	無条件に Link Aggregation Control Protocol（LACP）をイネーブルにします。
auto	Port Aggregation Protocol（PAgP）装置が検出された場合に限り、PAgP をイネーブルにします。
non-silent	（任意）PAgP 対応のパートナーに接続されたとき、インターフェイスを非サイレント動作に設定します。他の装置からのトラフィックが予想されている場合に PAgP モードで **auto** または **desirable** キーワードとともに使用されます。
desirable	無条件に PAgP をイネーブルにします。
on	オンモードをイネーブルにします。

passive	LACP 装置が検出された場合に限り、LACP をイネーブルにします。

コマンド デフォルト

チャネル グループは割り当てることができません。

モードは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 の EtherChannel では、チャネル グループに最初の物理ポートが追加されると、**channel-group** コマンドがポートチャネル インターフェイスを自動的に作成します。ポートチャネル インターフェイスを手動で作成する場合は、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用する必要はありません。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。

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

active モードは、ポートをネゴシエーション ステートにします。このステートでは、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。チャネルは、active モードまたは passive モードの別のポート グループで形成されます。

auto モードは、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありませ

ん。チャネルは、desirable モードの別のポート グループでだけ形成されます。auto がイネーブルの場合、サイレント動作がデフォルトになります。

desirable モードは、ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。EtherChannel は、desirable モードまたは auto モードの別のポート グループで形成されます。desirable がイネーブルの場合、サイレント動作がデフォルトになります。

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デバイス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、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。

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。

passive モードは、ポートをネゴシエーション ステートにします。この場合、ポートは受信した LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。チャネルは、active モードの別のポート グループでだけ形成されます。

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

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

アクティブまたはまだアクティブでない EtherChannel メンバとなっているポートを、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。

この例では、スタック内の 1 つのデバイスに 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 であるチャネル 5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/1 - 2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode desirable
Device(config-if-range)# end
```

この例では、スタック内の 1 つのデバイスに 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 であるチャネル 5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/1 - 2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

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

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/4 - 5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface GigabitEthernet 3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit
```

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

関連トピック

channel-protocol, （416 ページ）

interface port-channel, （431 ページ）

show etherchannel, （456 ページ）

show lacp, （460 ページ）

show pagp, （464 ページ）

channel-protocol

ポート上で使用されるプロトコルを制限してチャネリングを管理するには、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

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

pagp	Port Aggregation Protocol（PAgP）で EtherChannel を設定します。

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
Cisco IOS XE 3.2SE	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。

クロススタック構成の PAgP を設定できません。

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。

```
Device(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。

関連トピック

channel-group, （412 ページ）

show etherchannel, （456 ページ）

clear lacp

Link Aggregation Control Protocol（LACP）チャネル グループ 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**

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
counters	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
Cisco IOS XE 3.2SE	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 lacp counters** コマンドを使用します。また、指定のチャネル グループのカウンタのみをクリアするには、**clear lacp** *channel-group-number* **counters** コマンドを使用します。

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Device# 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。

```
Device# clear lacp 4 counters
```

情報が削除されたことを確認するには、**show lacp counters** または **show lacp** *channel-group-number* **counters** 特権 EXEC コマンドを入力します。

関連トピック

show lacp, （460 ページ）

clear pagp

Port Aggregation Protocol（PAgP）チャネル 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**

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
counters	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
Cisco IOS XE 3.2SE	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、指定したチャネル グループのカウンタのみをクリアできます。

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Device# 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。

```
Device# clear pagp 10 counters
```

情報が削除されたことを確認するには、**show pagp** 特権 EXEC コマンドを入力します。

関連トピック

debug pagp, （425 ページ）
show pagp, （464 ページ）

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

interface *interface-id*	（任意）指定のインターフェイスのスパニングツリーカウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN、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 ～ 128 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
Cisco IOS XE 3.2SE	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 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。

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。

```
Device# clear spanning-tree counters
```

関連トピック

clear spanning-tree detected-protocols, （421 ページ）

debug spanning-tree , （429 ページ）

clear spanning-tree detected-protocols

デバイスでプロトコル移行プロセスを再開して、強制的にネイバーと再ネゴシエーションするには、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）指定されたインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスとしては、物理ポート、VLAN、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 ～ 128 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
Cisco IOS XE 3.2SE	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（Rapid PVST+）プロトコルまたは Multiple Spanning Tree Protocol（MSTP）が稼働するデバイスは、組み込み済みのプロトコル移行方式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 デバイスと相互に動作できるようになります。Rapid PVST+ または MSTP デバイスが、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、そのデバイスはそのポートで IEEE 802.1D BPDU だけを送信します。マルチ スパニング ツリー（MST）デバイスが、レガシー BPDU、別のリージョンに対応する MST BPDU（バージョン 3）、または高速スパニング 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を検知します。

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

次の例では、ポートでプロトコル移行プロセスを再開する方法を示します。

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

関連トピック

clear spanning-tree detected-protocols, （421 ページ）

debug spanning-tree , （429 ページ）

debug etherchannel

EtherChannel 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。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

no debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

構文の説明

all	（任意）EtherChannel デバッグ メッセージをすべて表示します。
detail	（任意）EtherChannel デバッグ メッセージの詳細を表示します。
error	（任意）EtherChannel エラー デバッグ メッセージを表示します。
event	（任意）EtherChannel イベント メッセージを表示します。

idb	（任意）PAgP インターフェイス記述子ブロック デバッグ メッセージを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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 etherchannel コマンドは、**no debug etherchannel** コマンドと同じです。

（注） **linecard** キー ワードは、コマンドラインのヘルプに表示されますが、サポートされていません。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての EtherChannel デバッグ メッセージを表示する方法を示します。

```
Device# debug etherchannel all
```

次の例では、EtherChannel イベント関連のデバッグ メッセージを表示する方法を示します。

```
Device# debug etherchannel event
```

関連トピック

show etherchannel, （456 ページ）

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。LACP の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 lacp [**all | event | fsm | misc | packet**]

no debug lacp [**all | event | fsm | misc | packet**]

構文の説明

all	（任意）LACP デバッグ メッセージをすべて表示します。
event	（任意）LACP イベント デバッグ メッセージを表示します。
fsm	（任意） LACP有限状態マシン内の変更に関するメッセージを表示します。
misc	（任意）各種 LACP デバッグ メッセージを表示します。
packet	（任意）受信および送信 LACP 制御パケットを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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 etherchannel コマンドは、**no debug etherchannel** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権EXECモードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての LACP デバッグ メッセージを表示する方法を示します。

```
Device# debug LACP all
```

次の例では、LACPイベントに関連するデバッグ メッセージを表示する方法を示します。

```
Device# debug LACP event
```

debug pagp

Port Aggregation Protocol（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。PAgP の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 pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

構文の説明

all	（任意）PAgPデバッグメッセージをすべて表示します。
dual-active	（任意）デュアル アクティブ検出メッセージを表示します。
event	（任意）PAgP イベント デバッグ メッセージを表示します。
fsm	（任意）PAgP 有限状態マシン内の変更に関するメッセージを表示します。
misc	（任意）各種 PAgP デバッグ メッセージを表示します。
packet	（任意）送受信 PAgP 制御パケットを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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 pagp コマンドは、**no debug pagp** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての PAgP デバッグ メッセージを表示する方法を示します。

```
Device# debug pagp all
```

次の例では、PAgP イベントに関連するデバッグ メッセージを表示する方法を示します。

```
Device# debug pagp event
```

debug platform pm

プラットフォーム依存ポート 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には、このコマンドの **no** 形式を使用します。

debug platform pm {**all**| **counters**| **errdisable**| **fec**| **if-numbers**| **l2-control**| **link-status**| **platform**| **pm-spi**| **pm-vectors [detail]**| **ses**| **vlans**}

no debug platform pm {**all**| **counters**| **errdisable**| **fec**| **if-numbers**| **l2-control**| **link-status**| **platform**| **pm-spi**| **pm-vectors [detail]**| **ses**| **vlans**}

構文の説明

all	すべてのポート マネージャ デバッグ メッセージを表示します。
counters	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タを表示します。
errdisable	error-disabled 関連イベント デバッグ メッセージを表示します。

fec	転送等価クラス（FEC）プラットフォーム関連イベントデバッグ メッセージを表示します。
if-numbers	インターフェイス番号移動イベントデバッグ メッセージを表示します。
l2-control	レイヤ 2 制御インフラ デバッグ メッセージを表示します。
link-status	インターフェイス リンク検出イベント デバッグ メッセージを表示します。
platform	ポート マネージャ関数イベント デバッグ メッセージを表示します。
pm-spi	ポート マネージャ ステートフル パケット インスペクション（SPI）イベント デバッグ メッセージを表示します。
pm-vectors	ポート マネージャ ベクトル関連イベント デバッグ メッセージを表示します。
detail	（任意）ベクトル関数の詳細を表示します。
ses	サービス拡張シェルフ（SES）関連イベント デバッグ メッセージを表示します。
vlans	VLAN 作成および削除イベントデバッグ メッセージを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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 platform pm コマンドは、**no debug platform pm** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次に、VLAN の作成および削除に関するデバッグ メッセージを表示する例を示します。

```
Device# debug platform pm vlans
```

debug platform udld

プラットフォーム依存の単方向リンク検出（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 udld** コマンドを使用します。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 platform udld [**error**| **event**] [**switch** *switch-number*]

no debug platform udld [**error**| **event**] [**switch** *switch-number*]

構文の説明

error	（任意）エラー条件デバッグ メッセージを表示します。
event	（任意）UDLD 関連プラットフォーム イベント デバッグ メッセージを表示します。
switch *switch-number*	（任意）指定されたスタック メンバの UDLD デバッグ メッセージを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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 platform udld コマンドは、**no debug platform udld** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグを有効にする場合は、**session***switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

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、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には、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 | ha | mstp | pvst+| root | snmp | synchronization | switch | uplinkfast**}

no debug spanning-tree {**all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events | exceptions | general | mstp | pvst+| root | snmp | synchronization | switch | uplinkfast**}

構文の説明

all	スパニングツリーのデバッグ メッセージをすべて表示します。
backbonefast	BackboneFast イベント デバッグ メッセージを表示します。
bpdu	スパニングツリー 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。
bpdu-opt	最適化された BPDU 処理デバッグ メッセージを表示します。
config	スパニングツリー設定変更デバッグ メッセージを表示します。
etherchannel	EtherChannel サポート デバッグ メッセージを表示します。
events	スパニングツリー トポロジ イベント デバッグ メッセージを表示します。
exceptions	スパニングツリー例外デバッグ メッセージを表示します。
general	一般的なスパニングツリー アクティビティ デバッグ メッセージを表示します。

ha	高可用性スパニングツリー デバッグ メッセージを表示します。
mstp	Multiple Spanning Tree Protocol（MSTP）イベントをデバッグします。
pvst+	Per VLAN Spanning-Tree Plus（PVST+）イベント デバッグ メッセージを表示します。
root	スパニングツリー ルート イベント デバッグ メッセージを表示します。
snmp	スパニングツリーの Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）処理デバッグ メッセージを表示します。
switch	デバイス シム コマンド デバッグ メッセージを表示します。このシムは、一般的なスパニングツリー プロトコル（STP）コードと、各デバイス 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。
synchronization	スパニングツリー同期イベント デバッグ メッセージを表示します。
uplinkfast	UplinkFast イベント デバッグ メッセージを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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 spanning-tree コマンドは、**no debug spanning-tree** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべてのスパニングツリー デバッグ メッセージを表示する方法を示します。

```
Device# debug spanning-tree all
```

関連トピック

clear spanning-tree counters, （420 ページ）

clear spanning-tree detected-protocols, （421 ページ）

interface port-channel

ポートチャネルにアクセスするか、またはポートチャネルを作成するには、グローバル コンフィギュレーション モードで **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には、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

構文の説明

port-channel-number	チャネル グループ番号。指定できる範囲は 1 ～ 128 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
Cisco IOS XE 3.2SE	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。このコマンドでは、チャネル グループが最初の物理ポートを獲得すると、ポートチャネル論理インターフェイスが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。

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。

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設定してください。ポートチャネル インターフェイスでは設定できません。
- EtherChannel のアクティブ メンバであるポートを IEEE 802.1x ポートとしては設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、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。

次の例では、ポートチャネル番号 5 でポートチャネル インターフェイスを作成する方法を示します。

```
Device(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。

関連トピック

channel-group, （412 ページ）

show etherchannel, （456 ページ）

lacp max-bundle

ポート チャネルで許可されるアクティブ LACP ポートの最大数を定義するには、インターフェイス コンフィギュレーション モードで **lacp max-bundle** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp max-bundle *max_bundle_number*

no lacp max-bundle

構文の説明

max_bundle_number	ポート チャネルのアクティブ LACP ポートの最大数。指定できる範囲は 1 ～ 8 です。デフォルト値は 8 です。

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
Cisco IOS XE 3.3SE	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 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 個をホットスタンバイ 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デバイスは、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。他のデバイス上のポート プライオリティ（リンクの非制御側終端）は無視されます。

lacp max-bundle コマンドには、**port-channel min-links** コマンドで指定される数より大きい数を指定する必要があります。

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。

次に、ポート チャネル 2 で最大 5 個のアクティブ LACP ポートを指定する例を示します。

```
Device(config)# interface port-channel 2
Device(config-if)# lacp max-bundle 5
```

関連トピック

port-channel min-links, （445 ページ）

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
Cisco IOS XE 3.2SE	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 つのポートを active モードに、最大 8 つのポートを standby 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されます。

（注） LACP リンクを制御するデバイス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 デバイス 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。

物理ポート上での LACP の設定については、このリリースに対応する構成ガイドを参照してください。

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。

```
Device# interface gigabitethernet2/0/1
Device(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。

関連トピック

channel-group, （412 ページ）

lacp system-priority, （436 ページ）

show lacp, （460 ページ）

lacp rate

Link Aggregation Control Protocol（LACP）制御パケットが LACP がサポートされているインターフェイスに入力される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 **lacp rate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp rate {**normal**| **fast**}

no lacp rate

構文の説明

normal	LACP 制御パケットが通常レート（リンクのバンドル後、30 秒間隔）で入力されるように指定します。
fast	LACP 制御パケットが高速レート（1 秒に 1 回）で入力されるように指定します。

コマンド デフォルト

制御パケットのデフォルトの入力レートは、リンクがバンドルされた後、30 秒間隔です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	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 タイムアウトの期間を変更するには、このコマンドを使用します。シスコ スイッチの LACP タイムアウト値はインターフェイスで LACP レートの 3 倍に設定されます。**lacp rate** コマンドを使用して、スイッチの LACP タイムアウト値として 90 秒または 3 秒のいずれかを選択できます。

このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

次に、インターフェイス GigabitEthernet 0/0 の高速（1 秒）入力レートを指定する例を示します。

```
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# lacp rate fast
```

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、デバイスのグローバル 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

priority	LACP のシステム プライオリティ。指定できる範囲は 1 ～ 65535 です。

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
Cisco IOS XE 3.2SE	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 リンクのデバイスが判別されます。

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 つのポートを active モードに、最大 8 つのポートを standby 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デバイスは、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。他のデバイス上のポート 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。どちらのデバイスも同じ 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（デバイスの MAC アドレス）により制御するデバイスが判別されます。

lacp system-priority コマンドは、デバイス上のすべての 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。

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。

```
Device(config)# lacp system-priority 20000
```

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

関連トピック

channel-group, （412 ページ）

lacp port-priority, （434 ページ）

show lacp, （460 ページ）

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

aggregation-port	論理ポート チャネルでのアドレス ラーニングを指定します。デバイス は、EtherChannel のいずれかのポートを使用し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 ラーニングの場合、どの物理ポートにパケットが届くかは重要ではありません。
physical-port	EtherChannel 内の物理ポートでのアドレス ラーニングを指定します。デバイスは、送信元アドレスを学習した EtherChannel 内の同じポートを使用して送信元へパケットを送信します。チャネルのもう一方の終端では、特定の宛先 MAC または IP アドレスに対してチャネル内の同じポートが使用されます。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

学習方式は、リンクの両端で同一の設定にする必要があります。

コマンドライン インターフェイス（CLI）で **physical-port** キーワードが指定された場合でも、デバイス がサポートするのは集約ポートでのアドレス ラーニングのみです。**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドはデバイス のハードウェアには影響を及ぼしませんが、物理ポートによるアドレス ラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

デバイス 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物理ポート ラーナーとして デバイスを設定することを推奨します。また、**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 アドレスに基づいて負荷分散方式を設定すること

を推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような場合にのみ使用してください。

次の例では、EtherChannel 内の物理ポート上のアドレスを学習するように学習方式を設定する方法を示します。

```
Device(config-if)# pagp learn-method physical-port
```

次の例では、EtherChannel 内のポート チャネル上のアドレスを学習するように学習方式を設定する方法を示します。

```
Device(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。

関連トピック

pagp port-priority, （439 ページ）

show pagp, （464 ページ）

pagp port-priority

EtherChannel を経由してすべての Port Aggregation Protocol（PAgP）トラフィックが送信されるポートを選択するには、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。有効な範囲は 0 ～ 255 です。

コマンド デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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）で **physical-port** キーワードが指定された場合でも、デバイス がサポートするのは集約ポートでのアドレス ラーニングのみです。**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドはデバイス のハードウェアには影響を及ぼしませんが、Catalyst 1900 スイッチなど、物理ポートによるアドレス ラーニングのみをサポートするデバイスと PAgP の相互運用性を確保するために必要です。

デバイス 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物理ポート ラーナーとして デバイス を設定することを推奨します。また、**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 アドレスに基づいて負荷分散方式を設定することを推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような場合にのみ使用してください。

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。

```
Device(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。

関連トピック

pagp learn-method, （437 ページ）

port-channel load-balance, （442 ページ）

show pagp, （464 ページ）

port-channel

自動作成された EtherChannel を手動チャネルに変換して、設定を EtherChannel に追加するには、特権 EXEC モードで **port-channel** コマンドを使用します。

port-channel {*channel-group-number* **persistent** | **persistent** }

構文の説明

channel-group-number	チャネル グループ番号。指定できる範囲は 1 ～ 128 です。

persistent	自動作成された EtherChannel を手動チャネルに変更し、EtherChannel への設定の追加を許可します。

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
Cisco IOS XE 3.7.2E	このコマンドが導入されました。

使用上のガイドライン

EtherChannel の情報を表示するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

この例では、自動作成された EtherChannel を手動チャネルに変換する方法を示します。

```
Device# port-channel 1 persistent
```

port-channel auto

スイッチ上の Auto-LAG 機能をグローバルで有効にするには、グローバル コンフィギュレーション モードで **port-channel auto** コマンドを使用します。スイッチ上の Auto-LAG 機能をグローバルで無効にするには、このコマンドの **no** 形式を使用します。

port-channel auto

no port-channel 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

コマンド モード

デフォルトでは、Auto-LAG 機能がグローバルで無効にされ、すべてのポート インターフェイスで有効になっています。グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.2E	このコマンドが導入されました。

使用上のガイドライン

EtherChannel が自動作成されたかどうかを確認するには、**show etherchannel auto** 特権 EXEC コマンドを使用します。

次に、スイッチの Auto-LAG 機能を有効にする例を示します。

```
Device(config)# port-channel auto
```

port-channel load-balance

EtherChannel のポート間での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。ロードバランシング メカニズム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。

port-channel load-balance {**dst-ip**| **dst-mac**| **dst-mixed-ip-port**| **dst-port**| **extended**| **src-dst-ip**| **src-dst-mac**| **src-dst-mixed-ip-port**| **src-dst-port**| **src-ip**| **src-mac**| **src-mixed-ip-port**| **src-port**}

no port-channel load-balance

構文の説明

dst-ip	宛先ホストの IP アドレスに基づいた負荷分散を指定します。
dst-mac	宛先ホストの MAC アドレスに基づいた負荷分散を指定します。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ネルの異なるポートに送信されます。
dst-mixed-ip-port	宛先 IPv4 または IPv6 アドレスと TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
dst-port	宛先 TCP/UDP（レイヤ 4）と IPv4 と IPv6 の両方のポート番号に基づいて負荷分散を指定します。
extended	EtherChannel のポート間の拡張ロード バランス方式を設定します。**port-channel load-balance extended** コマンドを参照してください。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいて負荷分散を指定します。

src-dst-mac	送信元および宛先ホストのMACアドレスに基づいた負荷分散を指定します。
src-dst-mixed-ip-port	送信元および宛先のホスト IP アドレスと TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
src-dst-port	送信元および宛先の TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散を指定します。
src-mac	送信元のMACアドレスに基づいた負荷分散を指定します。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。
src-mixed-ip-port	送信元ホスト IP アドレスと TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
src-port	TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。

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
Cisco IOS XE 3.2SE	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。

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。

```
Device(config)# port-channel load-balance dst-mac
```

port-channel load-balance extended

EtherChannelのポート間での負荷分散方式の組み合わせを設定するには、グローバル コンフィギュレーション モードで **port-channel load-balance extended** コマンドを使用します。ロードバランシング メカニズム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。

port-channel load-balance extended[**dst-ip**| **dst-mac**| **dst-port**| **ipv6-label**| **l3-proto**| **src-ip**| **src-mac**| **src-port**]

no port-channel load-balance extended

構文の説明

dst-ip	（任意）宛先ホストの IP アドレスに基づいて負荷分散を指定します。
dst-mac	（任意）宛先ホストの MAC アドレスに基づいて負荷分散を指定します。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ネルの異なるポートに送信されます。
dst-port	（任意）IPv4 と IPv6 両方の宛先 TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
ipv6-label	（任意）送信元 MAC アドレスと IPv6 フロー ラベルに基づいて負荷分散を指定します。
l3-proto	（任意）送信元 MAC アドレスとレイヤ 3 プロトコルに基づいて負荷分散を指定します。
src-ip	（任意）送信元ホストの IP アドレスに基づいて負荷分散を指定します。
src-mac	（任意）送信元の MAC アドレスに基づいて負荷分散を指定します。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。
src-port	（任意）TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

どのような場合にこれらの転送方式を使用するかについては、このリリースの*Layer 2/3 Configuration Guide (Catalyst 3850 Switches)*を参照してください。

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。

次に、拡張負荷分散方式を設定する例を示します。

```
Device(config)# port-channel load-balance extended dst-ip dst-mac src-ip
```

port-channel min-links

ポート チャネルがアクティブになるように、リンクアップ状態で、EtherChannel にバンドルする必要がある LACP ポートの最小数を定義するには、インターフェイス コンフィギュレーション モードで **port-channel min-links** を使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel min-links *min_links_number*

no port-channel min-links

構文の説明

min_links_number	ポート チャネル内のアクティブな LACP ポートの最小数。指定できる範囲は 2 ～ 8 です。デフォルトは 1 です。

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
Cisco IOS XE 3.3SE	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 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 個をホットスタンバイ 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デバイスは、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。他のデバイス上のポート プライオリティ（リンクの非制御側終端）は無視されます。

port-channel min-links コマンドには、**lacp max-bundle** コマンドで指定される数より少ない数を指定する必要があります。

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。

次に、ポート チャネル 2 がアクティブになる前に、少なくとも 3 個のアクティブな LACP ポートを指定する例を示します。

```
Device(config)# interface port-channel 2
Device(config-if)# port-channel min-links 3
```

関連トピック

lacp max-bundle, （432 ページ）

rep admin vlan

Resilient Ethernet Protocol（REP） の 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。VLAN 1 が管理 VLAN になるようにデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

rep admin vlan *vlan-id*

no rep admin vlan

構文の説明

vlan-id	48 ビット スタティック MAC アドレス。

コマンド デフォルト

管理 VLAN のデフォルト値は VLAN 1（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	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 管理 VLAN の範囲は 2 ～ 4094 です。

管理 VLAN を設定しない場合、デフォルト VLAN は VLAN 1 です。デフォルトの VLAN 1 は常に設定されています。ルータとセグメント上には管理 VLAN は 1 つだけとなります。

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。

次に、VLAN 100 を REP 管理 VLAN として設定する例を示します。

```
Device(config)#  rep admin vlan 100
```

rep block port

REP プライマリ エッジ ポートで REP VLAN ロード バランシングを設定するには、インターフェイス コンフィギュレーション モードで **rep block port** コマンドを使用します。VLAN 1 が管理 VLAN になるようにデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

rep block port {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}

no rep block port {**id** *port-id* | *neighbor-offset* | **preferred**}

構文の説明

id *port-id*	REP を有効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。特権 EXEC モードで **show interface** *interface-id* **rep detail** コマンドを入力すると、インターフェイスのポート ID を表示できます。
neighbor-offset	ネイバーのオフセット番号を入力することで、VLANブロック代替ポートを識別します。指定できる範囲は –256 ～ +256 で、値 0 は無効です。
preferred	すでに VLAN ロード バランシングの優先代替ポートとして指定されている通常セグメント ポートを選択します。
vlan	ブロックされる VLAN を指定します。
vlan-list	表示される VLAN ID または VLAN ID の範囲。ブロックする VLAN ID（1 ～ 4094 の範囲）を入力するか、ブロックする LAN ID の範囲または連続番号（1-3、22、41-44 など）を入力します。

all	すべての VLAN をブロックします。

コマンド デフォルト

特権 EXEC モードで **rep preempt segment** コマンドを入力した後のデフォルト動作では（手動プリエンプションの場合）、プライマリ エッジ ポートで VLAN すべてをブロックします。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プションなし、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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、REP プライマリ エッジ ポート上に入力する必要があります。

オフセット番号を入力して代替ポートを選択する場合、オフセット番号はエッジポートのダウンストリーム ネイバー ポートを識別します。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負の番号は、セカンダリ エッジポート（オフセット番号–1）とダウンストリーム ネイバーを識別します。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。

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 seconds** コマンドを入力することでプリエンプション遅延時間を設定しており、リンク障害とリカバリが発生した場合、別のリンク障害が発生することなく設定したプリエンプション期間が経過すると、VLAN ロード バランシングが開始されます。ロードバランシング設定で指定された代替ポートは、設定された VLAN をブロックし、その他すべてのセグメント ポートのブロックを解除します。プライマリ エッジ ポートで VLAN バランシングの代替ポートを決定できない場合、デフォルトのアクションはプリエンプ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。ポートのポート ID を判別するには、特権 EXEC モードで、 **show interfaces** *interface-id* **rep detail** コマンドを入力します。

次に、REP VLAN ロード バランシングを設定する例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep block port id 0009001818D68700 vlan 1-100
```

rep lsl-age-timer

REP リンク ステータス レイヤ（LSL）のエージアウト タイマー値を設定するには、インターフェイス コンフィギュレーション モードで **rep lsl-age-timer** コマンドを使用します。デフォルトのエージアウト タイマー値に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-age-timer *milliseconds*

no rep lsl-age-timer *milliseconds*

構文の説明

milliseconds	ミリ秒単位の REP LSL エージアウト タイマー値。範囲は 120 ～ 10000 ミリ秒で、40 ミリ秒の倍数を指定します。

コマンド デフォルト

デフォルトの LSL エージアウト タイマー値は 5 ミリ秒です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	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 lsl-age-timer コマンドは、REP LSL エージアウト タイマー値を設定するために使用されます。REP の設定可能なタイマーを設定する際には、最初に REP LSL の再試行回数を設定し、その後、REP LSL のエージアウト タイマー値を設定することを推奨します。

次に、REP LSL エージアウト タイマー値を設定する例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 1 edge primary
Device(config-if)#  rep lsl-age-timer 2000
```

rep lsl-retries

REP リンク ステータス レイヤ（LSL）の再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 **rep lsl-retries** コマンドを使用します。デフォルトの再試行回数に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-retries *number-of-retries*

no rep lsl-retries *number-of-retries*

構文の説明

number-of-retries	LSL の再試行回数。再試行回数の範囲は、3 ～ 10 です。

コマンド デフォルト

デフォルトの再試行回数は 5 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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	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 lsl-retries コマンドは、REP リンクを無効にする前に再試行回数を設定するために使用されます。REP の設定可能なタイマーを設定する際には、最初に REP LSL の再試行回数を設定し、その後、REP LSL のエージアウト タイマー値を設定することを推奨します。

次に、REP LSL の再試行回数を設定する例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 2 edge primary
```

rep preempt delay

セグメント ポートの障害およびリカバリの発生後、REP VLAN ロード バランシングがトリガーされるまでの待機時間を設定するには、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。設定した遅延を削除するには、このコマンドの **no** 形式を使用します。

rep preempt delay *seconds*

no rep preempt delay

構文の説明

seconds	REP プリエンプションを遅延する秒数です。範囲は 15 ～ 300 秒です。デフォルトは遅延なしの手動プリエンプションです。

コマンド デフォルト

REP プリエンプション遅延は設定されていません。デフォルトは遅延なしの手動プリエンプションです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、REP プライマリ エッジ ポート上に入力する必要があります。

リンク障害とリカバリ後に自動的にVLANロードバランシングをトリガーする場合、このコマンドを入力してプリエンプション時間遅延を設定する必要があります。

VLANロードバランシングが設定されている場合、セグメントポート障害とリカバリの後、VLANロード バランシングが発生する前に REP プライマリ エッジ ポートで遅延タイマーが起動されます。各リンク障害が発生した後にタイマーが再起動することに注意してください。タイマーが満了となると、（**rep block port** インターフェイス コンフィギュレーション コマンドを使用して設定された）VLAN ロード バランシングを実行するように REP プライマリ エッジが代替ポートに通知し、新規トポロジ用のセグメントが準備されます。設定された VLAN リストは代替ポートでブロックされ、他のすべての VLAN はプライマリ エッジ ポートでブロックされます。

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。

次に、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 秒に設定する例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep preempt delay 100
```

rep preempt segment

セグメントで REP VLAN ロード バランシングを手動で開始するには、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プションです。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが追加されました。

使用上のガイドライン

ルータのプライマリ エッジ ポートがあるセグメントで、次のコマンドを入力します。

VLAN ロード バランシングのプリエンプションを設定する前に、他のすべてのセグメントの設定が完了していることを確認してください。VLAN ロード バランシングのプリエンプションはネットワークを中断する可能性があるため、**rep preempt segment** *segment-id* コマンドを入力すると、このコマンドの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 ポートで、インターフェイス コンフィギュレーション モードから **rep preempt delay** *seconds* コマンドを入力せずに、プリエンプション時間遅延を設定する場合、デフォルト設定はセグメントでの VLAN ロード バランシングの手動トリガーです。 **show rep topology** 特権 EXEC コマンドを使用して、セグメント内のどのポートがプライマリ エッジ ポートであるかを確認します。

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）。

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** コマンドを入力して VLAN ロードバランシングを設定してから、手動でプリエンプションを開始します。

次に、セグメント 100 で REP プリエンプションを手動でトリガーする例を示します。

```
Device#  rep preempt segment 100
```

rep segment

インターフェイスで REP を有効にし、そのインターフェイスにセグメント 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 を無効にするには、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

segment-id	REP が有効になっているセグメント。セグメント ID をインターフェイスに割り当てます。有効な範囲は 1 ～ 1024 です。
edge	（任意）エッジ ポートとしてポートを設定します。各セグメントにあるエッジ ポートは 2 つだけです。
no-neighbor	（任意）セグメント エッジを外部 REP ネイバーなしに指定します。
primary	（任意）プライマリ エッジ ポート（VLAN ロード バランシングを設定できるポート）としてポートを指定します。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。
preferred	（任意）ポートを優先代替ポートまたは VLAN ロードバランシングの優先ポートに指定します。 （注） ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。

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。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	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 IEEE 802.1Q または 802.1AD ポートのいずれかである必要があります。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。

REP がルータの 2 つのポートでイネーブルの場合、両方のポートが通常セグメント ポートまたはエッジ ポートである必要があります。REP ポートは以下の規則に従います。

- 1 つのルータ上で 1 つのポートだけがセグメントで設定される場合、このポートは 1 つのエッジ ポートである必要があります。
- 1 つのルータ上で 2 つのポートが同じセグメントに属する場合、どちらのポートも通常セグメント ポートである必要があります。
- 1 つのルータ上で 2 つのポートが同じセグメントに属し、1 つがエッジ ポートとして設定され、もう 1 つが通常のセグメント ポートとして設定された場合（設定ミス）、エッジ ポートは通常セグメント ポートとして処理されます。

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。

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。

次に、通常（非エッジ）セグメント ポートで REP を有効にする例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 100
```

次に、ポートで REP を有効にし、そのポートを REP プライマリ エッジ ポートとして指定する例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 100 edge primary
```

次に、ポートで REP を有効にし、そのポートを REP セカンダリ エッジ ポートとして指定する例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 100 edge
```

次に、REP をネイバーなしの エッジ ポートとして有効にする例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 1 edge no-neighbor primary
```

rep stcn

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または他のセグメントに送信するように REP エッジ 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 **rep stcn** コマンドを使用します。インターフェイスまたはセグメントへの STCN の送信を無効にするには、このコマンドの **no** 形式を使用します。

rep stcn {**interface** *interface-id* | **segment** *segment-id-list*}

no rep stcn {**interface** | **segment**}

構文の説明

interface *interface-id*	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。
segment *segment-id-list*	STCN を受信する 1 つの REP セグメントまたはセグメントの一覧を指定します。セグメントの範囲は 1 ～ 1024 です。また、一連のセグメント（たとえば 3 ～ 5、77、100）を設定することもできます。

コマンド デフォルト

他のインターフェイスおよびセグメントへの STCN 送信は、無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが追加されました。

使用上のガイドライン

1 つ以上のセグメントまたはインターフェイスに STCN を送信するには、セグメント エッジ ポートで次のコマンドを入力します。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。

次に、セグメント 25 ～ 50 に STCN を送信するように REP エッジ ポートを設定する例を示します。

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#   rep stcn segment 25-50
```

show etherchannel

チャネルの EtherChannel 情報を表示するには、ユーザ 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**}] | [**auto**| **detail**| **load-balance**| **port**| **port-channel**| **protocol**| **summary**]

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
auto	（任意）Etherchannel が自動的に作成する情報を表示します。
detail	（任意）詳細な EtherChannel 情報を表示します。
load-balance	（任意）ポート チャネル内のポート間の負荷分散方式、またはフレーム配布方式を表示します。
port	（任意）EtherChannel ポートの情報を表示します。
port-channel	（任意）ポート チャネル情報を表示します。
protocol	（任意）EtherChannel で使用されるプロトコルを表示します。
summary	（任意）各チャネル グループのサマリーを 1 行で表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

チャネル グループ番号を指定しない場合は、すべてのチャネル グループが表示されます。

次の例では、**show etherchannel auto** コマンドの出力を示します。

```
デバイス# show etherchannel auto
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SUA)        LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

次の例では、**show etherchannel** *channel-group-number* **detail** コマンドの出力を示します。

```
Device> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:      LACP
                    Ports in the group:
                    -------------------
Port: Gi1/0/1
------------
Port state    = Up Mstr In-Bndl
Channel group = 1         Mode  = Active        Gcchange = -
Port-channel  =           Po1GC = -             Pseudo port-channel = Po1
Port index    =           0Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
       A - Device is in active mode.        P - Device is in passive mode.

Local information:
                         LACP port   Admin   Oper   Port   Port
Port     Flags   State   Priority    Key     Key    Number State
Gi1/0/1   SA      bndl     32768      0x1     0x1    0x101  0x3D
Gi1/0/2    A      bndl     32768      0x0     0x1    0x0    0x3D

Age of the port in the current state: 01d:20h:06m:04s

                   Port-channels in the group:
                   ----------------------

Port-channel: Po1   (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load   Port      EC state        No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1    Active           0
 0      00    Gi1/0/2    Active           0
```

```
Time since last port bundled:   01d:20h:24m:44s   Gi1/0/2
```

次の例では、**show etherchannel** *channel-group-number* **summary** コマンドの出力を示します。

```
Device> show etherchannel 1 summary
Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       u - unsuitable for bundling
       U - in use f - failed to allocate aggregator
       d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
 1     Po1(SU)       LACP        Gi1/0/1(P) Gi1/0/2(P)
```

次の例では、**show etherchannel** *channel-group-number* **port-channel** コマンドの出力を示します。

```
Device> 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
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load   Port   EC state           No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1 Active             0
 0      00    Gi1/0/2 Active             0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

次の例では、**show etherchannel protocol** コマンドの出力を示します。

```
Device# show etherchannel protocol
Channel-group listing:
-----------------------
Group: 1
----------
Protocol: LACP
Group: 2
----------
Protocol: PAgP
```

関連トピック

channel-group, （412 ページ）

channel-protocol, （416 ページ）

interface port-channel, （431 ページ）

show interfaces rep detail

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詳細な REP 設定とステータス（管理 VLAN を含む）を表示するには、特権 EXEC モードで **show interfaces rep detail** コマンドを使用します。

show interfaces [*interface-id*] **rep detail**

構文の説明

interface-id	（任意）ポート ID を表示するために使用される物理インターフェイス。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	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、1 つ以上のセグメントまたは 1 つのインターフェイスに STCN を送信先するために、セグメント エッジ ポートで入力します。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。

次に、指定されたインターフェイスに関する REP 設定とステータスを表示する例を示します。

```
Device#  show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
```

```
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

show lacp

Link Aggregation Control Protocol（LACP）チャネル グループ情報を表示するには、ユーザ 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

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィック情報を表示します。
internal	内部情報を表示します。
neighbor	ネイバーの情報を表示します。
sys-id	LACPによって使用されるシステム識別子を表示します。システム識別子は、LACP システム プライオリティと デバイス MAC アドレスで構成されています。

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
Cisco IOS XE 3.2SE	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、アクティブなチャネル グループの情報が表示されます。特定のチャネル情報を表示するには、チャネル グループ番号を指定して **show lacp** コマンドを入力します。

チャネル グループを指定しない場合は、すべてのチャネル グループが表示されます。

channel-group-number を入力すると、**sys-id** 以外のすべてのキーワードでチャネル グループを指定できます。

次の例では、**show lacp counters** ユーザ EXEC コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device> show lacp counters
              LACPDUs         Marker      Marker Response   LACPDUs
Port        Sent  Recv      Sent  Recv      Sent  Recv      Pkts  Err
--------------------------------------------------------------------
Channel group:1
Gi2/0/1       19    10         0    0          0    0         0
Gi2/0/2       14    6          0    0          0    0         0
```

表 *24*：*show lacp counters* のフィールドの説明

フィールド	説明
LACPDUs Sent および Recv	ポートによって送受信された LACP パケット数
Marker Sent および Recv	ポートによって送受信された LACP Marker パケット数
Marker Response Sent および Recv	ポートによって送受信された LACP Marker 応答パケット数
LACPDUs Pkts および Err	ポートの LACP によって受信された、未知で不正なパケット数

次の例では、**show lacp internal** コマンドの出力を示します。

```
Device> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Gi2/0/1    SA      bndl      32768         0x3       0x3       0x4    0x3D
Gi2/0/2    SA      bndl      32768         0x3       0x3       0x5    0x3D
```

次の表に、出力されるフィールドの説明を示します。

表 *25*：*show lacp internal* のフィールドの説明

フィールド	説明
State	特定のポートの状態。次に使用可能な値を示します。 • –：ポートの状態は不明です。 • **bndl**：ポートがアグリゲータに接続され、他のポートとバンドルされています。 • **susp**：ポートが中断されている状態で、アグリゲータには接続されていません。 • **hot-sby**：ポートがホットスタンバイの状態です。 • **indiv**：ポートは他のポートとバンドルできません。 • **indep**：ポートは独立状態です。バンドルされていませんが、データ トラフィックを処理することができます。この場合、LACP は相手側ポートで実行されていません。 • **down**：ポートがダウンしています。
LACP Port Priority	ポートのプライオリティ設定。ハードウェアの制限により互換性のあるすべてのポートを集約できない場合、LACP はポート プライオリティを使用し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。ポートが他のポートと集約できるかどうかは、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）と設定に指定された制限によって決定されます。
Oper Key	ポートで使用される実行時の操作キー。LACP は自動的に値を生成します（16 進数）。
Port Number	ポート番号。

フィールド	説明
Port State	ポートの状態変数。1 つのオクテット内で個々のビットとしてエンコードされ、次のような意味になります。 • bit0：LACP のアクティビティ • bit1：LACP のタイムアウト • bit2：集約 • bit3：同期 • bit4：収集 • bit5：配信 • bit6：デフォルト • bit7：期限切れ （注） 上のリストでは、bit7 が MSB で bit0 は LSB です。

次の例では、**show lacp neighbor** コマンドの出力を示します。

```
Device> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
       A - Device is in Active mode        P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner                 Partner               Partner
Port      System ID               Port Number   Age     Flags
Gi2/0/1   32768,0007.eb49.5e80    0xC             19s    SP

          LACP Partner            Partner       Partner
          Port Priority           Oper Key      Port State
          32768                   0x3           0x3C

Partner's information:

          Partner                 Partner               Partner
Port      System ID               Port Number   Age     Flags
Gi2/0/2   32768,0007.eb49.5e80    0xD             15s    SP

          LACP Partner            Partner       Partner
          Port Priority           Oper Key      Port State
          32768                   0x3           0x3C
```

次の例では、**show lacp sys-id** コマンドの出力を示します。

```
Device> show lacp sys-id
32765,0002.4b29.3a00
```

システム ID は、システム プライオリティおよびシステム MAC アドレスで構成されています。最初の 2 バイトはシステム プライオリティ、最後の 6 バイトはグローバルに管理されているシステム関連の個々の MAC アドレスです。

関連トピック

clear lacp, （418 ページ）

lacp port-priority, （434 ページ）

lacp system-priority, （436 ページ）

show pagp

Port Aggregation Protocol（PAgP; ポート集約プロトコル）のチャネル 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

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィック情報を表示します。
dual-active	デュアルアクティブ ステータスが表示されます。
internal	内部情報を表示します。
neighbor	ネイバーの情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、アクティブなチャネル グループの情報が表示されます。非アクティブ ポート チャネルの情報を表示するには、チャネル グループ番号を指定して **show pagp** コマンドを入力します。

次の例では、**show pagp 1 counters** コマンドの出力を示します。

```
Device> show pagp 1 counters
              Information        Flush
Port          Sent   Recv     Sent   Recv
--------------------------------------
Channel group: 1
  Gi1/0/1     45     42       0      0
  Gi1/0/2     45     41       0      0
```

次の例では、**show pagp dual-active** コマンドの出力を示します。

```
Device> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi1/0/1   No              デバイス              Gi3/0/3   N/A
Gi1/0/2   No              デバイス              Gi3/0/4   N/A

<output truncated>
```

次の例では、**show pagp 1 internal** コマンドの出力を示します。

```
Device> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/1     SC    U6/S7   H       30s      1        128        Any     16
Gi1/0/2     SC    U6/S7   H       30s      1        128        Any     16
```

次の例では、**show pagp 1 neighbor** コマンドの出力を示します。

```
Device> show pagp 1 neighbor

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.

Channel group 1 neighbors
            Partner              Partner          Partner           Partner Group
Port        Name                 Device ID        Port         Age  Flags   Cap.
Gi1/0/1     デバイス-p2           0002.4b29.4600   Gi01//1        9s SC      10001
Gi1/0/2     デバイス-p2           0002.4b29.4600   Gi1/0/2       24s SC      10001
```

関連トピック

clear pagp, （419 ページ）

show platform etherchannel

プラットフォーム依存 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 *channel-group-number* {**group-mask**| **load-balance mac** *src-mac dst-mac* [**ip** *src-ip dst-ip* [**port** *src-port dst-port*]]} [**switch** *switch-number*]

構文の説明

channel-group-number	チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
group-mask	EtherChannel グループ マスクを表示します。
load-balance	EtherChannel ロード バランシングのハッシュ アルゴリズムをテストします。
mac *src-mac dst-mac*	送信元と宛先の MAC アドレスを指定します。
ip *src-ip dst-ip*	（任意）送信元と宛先の IP アドレスを指定します。
port *src-port dst-port*	（任意）送信元と宛先のレイヤ ポート番号を指定します。
switch *switch-number*	（任意）スタック メンバを指定します。

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
Cisco IOS XE 3.2SE	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。

show platform pm

プラットフォーム依存のポート 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 {**etherchannel** *channel-group-number* **group-mask**| **interface-numbers**| **port-data** *interface-id*| **port-state**| **spi-info**| **spi-req-q**}

構文の説明

etherchannel *channel-group-number* **group-mask**	指定されたチャネル グループの EtherChannel グループ マスク テーブルを表示します。指定できる範囲は 1 ～ 128 です。
interface-numbers	インターフェイス番号情報を表示します。
port-data *interface-id*	指定されたインターフェイスのポートデータ情報を表示します。
port-state	ポートの状態情報を表示します。
spi-info	ステートフル パケット インスペクション（SPI）情報を表示します。
spi-req-q	確認応答のためのステートフル パケット インスペクション（SPI）の最大待機時間を表示します。

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
Cisco IOS XE 3.2SE	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。

show rep topology

1 セグメントまたは全セグメントの REP トポロジ情報（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）を表示するには、特権 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 *segment-id*	（任意）REP トポロジ情報を表示するセグメントを指定します。指定できる ID 範囲は 1 ～ 1024 です。
archive	（任意）セグメントの前のトポロジを表示します。このキーワードは、リンク障害のトラブルシューティングに役立ちます。
detail	（任意）REP トポロジの詳細情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが追加されました。

次に、show rep topology コマンドの出力例を示します。

```
Device#  show rep topology

REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Te5/4      Pri  Open
10.64.106.228    Te3/4           Open
10.64.106.228    Te3/3           Open
10.64.106.67     Te4/3           Open
10.64.106.67     Te4/4           Alt
10.64.106.63     Te4/4      Sec  Open

REP Segment 3
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Gi50/1     Pri  Open
SVT_3400_2       Gi0/3           Open
SVT_3400_2       Gi0/4           Open
10.64.106.68     Gi40/2          Open
10.64.106.68     Gi40/1          Open
10.64.106.63     Gi50/2     Sec  Alt
```

次に、**show rep topology detail** コマンドの出力例を示します。

```
Device#  show rep topology detail

REP Segment 1
10.64.106.63, Te5/4 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
  Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
  Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 6 / [-1]
```

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）の管理ステータスおよび運用ステータスを表示するには、ユーザ EXEC モードで **show udld** コマンドを使用します。

show udld [**Auto-Template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan**] *interface_number*

show udld neighbors

構文の説明

Auto-Template	（任意）自動テンプレートインターフェイスのUDLD動作ステータスを表示します。範囲は 1 ～ 999 です。
Capwap	（任意）CAPWAPインターフェイスのUDLD動作ステータスを表示します。指定できる範囲は0～2147483647です。
GigabitEthernet	（任意）GigabitEthernet インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
GroupVI	（任意）グループ仮想インターフェイスの UDLD 動作ステータスを表示します。範囲は 1 ～ 255 です。
InternalInterface	（任意）内部インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
Loopback	（任意）ループバック インターフェイスのUDLD動作ステータスを表示します。指定できる範囲は0～2147483647です。
Null	（任意）null インターフェイスの UDLD 動作ステータスを表示します。
Port-channel	（任意）イーサネット チャネル インターフェイスの UDLD 動作ステータスを表示します。有効な範囲は 1 ～ 128 です。
TenGigabitEthernet	（任意）10 ギガビット イーサネット インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
Tunnel	（任意）トンネルインターフェイスのUDLD動作ステータスを表示します。指定できる範囲は0～2147483647です。

Vlan	（任意）VLAN インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 1 ～ 4095 です。
interface-id	（任意）インターフェイスの ID およびポート番号です。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。
neighbors	（任意）ネイバー情報だけを表示します。

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
Cisco IOS XE 3.2SE	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 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。

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。次の表に、この出力で表示されるフィールドについて説明します。

```
Device> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
```

```
CDP Device name: Switch-A
```

表 *26* : ***show udld*** のフィールドの説明

フィールド	説明
Interface	UDLD に設定されたローカル デバイスのインターフェイス。
Port enable administrative configuration setting	ポートでの UDLD の設定方法。UDLD がイネーブルまたはディセーブルの場合、ポートのイネーブル設定は運用上のイネーブル ステートと同じです。それ以外の場合、イネーブル動作設定は、グローバルなイネーブル設定によって決まります。
Port enable operational state	このポートで UDLD が実際に稼働しているかどうかを示す動作ステート。
Current bidirectional state	リンクの双方向ステート。リンクがダウンしているか、または UDLD 非対応デバイスに接続されている場合は、unknown ステートが表示されます。リンクが UDLD 対応デバイスに通常どおり双方向接続されている場合は、bidirectional ステートが表示されます。その他の値が表示されている場合は、正しく配線されていません。
Current operational state	UDLD ステートマシンの現在のフェーズ。通常の双方向リンクの場合、多くは、ステートマシンはアドバタイズ フェーズです。
Message interval	ローカル デバイスからアドバタイズ メッセージを送信する頻度。単位は秒です。
Time out interval	検出ウィンドウ中に、UDLD がネイバー デバイスからのエコーを待機する期間（秒）。
Entry 1	最初のキャッシュ エントリの情報。このエントリには、ネイバーから受信されたエコー情報のコピーが格納されます。
Expiration time	このキャッシュ エントリの期限が切れるまでの存続期間（秒）。
Device ID	ネイバー デバイスの ID。

フィールド	説明
Current neighbor state	ネイバーの現在の状態。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（Switch）に設定されている場合、システムのシリアル番号が表示されます。
Port ID	UDLD に対してイネーブルに設定されたネイバーのポート ID。
Neighbor echo 1 device	エコーの送信元であるネイバーのネイバーデバイス名。
Neighbor echo 1 port	エコーの送信元であるネイバーのポート番号 ID。
Message interval	ネイバーがアドバタイズメッセージを送信する速度（秒）。
CDP device name	CDPデバイス名またはシステム シリアル番号。装置名が設定されていないか、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。

次の例では、**show udld neighbors** コマンドの出力を示します。

```
Device# show udld neighbors
Port     Device Name          Device ID  Port-ID  OperState
-------- -------------------- ---------- -------- --------------
Gi2/0/1  Switch-A             1          Gi2/0/1  Bidirectional
Gi3/0/1  Switch-A             2          Gi3/0/1  Bidirectional
```

関連トピック

udld, （484 ページ）

udld port, （486 ページ）

udld reset, （488 ページ）

switchport

レイヤ 3 モードになっているインターフェイスをレイヤ 2 設定用のレイヤ 2 モードに配置するには、インターフェイス コンフィギュレーション モードで **switchport** コマンドを使用します。インターフェイスをレイヤ 3 モードに配置するには、このコマンドの **no** 形式を使用します。

switchport

no switchport

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、すべてのインターフェイスがレイヤ 2 モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

インターフェイスをルーテッド インターフェイスの状態に設定して、レイヤ 2 の設定をすべて削除するには、**no switchport** コマンド（パラメータの指定なし）を使用します。このコマンドは、ルーテッド ポートに IP アドレスを割り当てる前に使用する必要があります。

（注） このコマンドは、LAN Base 機能セットを実行しているデバイスではサポートされません。

no switchport コマンドを入力するとポートがシャットダウンされて、その後再び有効になります。その際に、ポートの接続先のデバイスでメッセージが生成されることがあります。

レイヤ 2 モードからレイヤ 3 モード（またはその逆）にインターフェイスを変更すると、影響を受けたインターフェイスに関連する以前の設定情報が失われる可能性があり、インターフェイスがデフォルト設定に戻ります。

（注） インターフェイスがレイヤ 3 インターフェイスとして設定されている場合、最初に **switchport** コマンドを入力して、そのインターフェイスをレイヤ 2 ポートとして設定する必要があります。その後、**switchport access vlan** コマンドと **switchport mode** コマンドを入力できます。

switchport コマンドは、シスコ ルーテッド ポートをサポートしないプラットフォームでは使用されません。このようなプラットフォーム上のすべての物理ポートは、レイヤ 2 のスイッチド インターフェイスとして想定されます。

インターフェイスのポート ステータスを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

次の例では、インターフェイスをレイヤ2ポートとして運用することを中止し、シスコのルーテッド ポートにする方法を示します。

```
Device(config-if)# no switchport
```

次の例では、ポートのインターフェイスをシスコのルーテッド ポートとして運用することを中止し、レイヤ 2 のスイッチド インターフェイスに変更する方法を示します。

```
Device(config-if)# switchport
```

switchport access vlan

ポートをスタティック アクセス ポート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 **switchport access vlan** コマンドを使用します。デバイスのアクセス モードをデフォルトの VLAN モードにリセットするには、このコマンドの **no** 形式を使用します。

switchport access vlan {*vlan-id*| **name***vlan_name*}

no switchport access vlan

構文の説明

vlan-id	アクセス モード VLAN のVLAN ID。範囲は 1 ~ 4094。

コマンド 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。

コマンド モード

インターフェイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	**name** *vlan_name* キーワードが導入されました。

使用上のガイドライン

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。

スイッチポートのモードが **access vlan** *vlan-id* に設定されている場合、ポートは指定された VLAN のメンバとして動作します。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。

no switchport access コマンドを使用すると、アクセス モード VLAN がデバイスに適したデフォルト VLAN にリセットされます。

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。

```
Device(config-if)# switchport access vlan 2
```

次の例では、最初に VLAN ID と VLAN 名を対応させて、その情報を VLAN データベースに格納し、その後、アクセス モードにあるインターフェイス上の VLAN を設定します（名前を使用）。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、Access Mode VLAN: 行の情報を調べます。

手順 1：VLAN データベースでのエントリの作成

```
Device# configure terminal
Device(config)# vlan 33
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

手順 2：VLAN データベースの確認

```
Device # show vlan id 33
VLAN  Name   Status   Ports
---- -------------------------------- --------- -------------------------------

33    test   active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
33   enet  100033     1500   -      -      -        -   -       0      0

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary Type              Ports
------- --------- --------------- -----------------------------------------
```

手順 3：VLAN 名を使用したインターフェイスへの VLAN の割り当て

```
Device # configure terminal
Device(config)# interface GigabitEthernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan name test
Device(config-if)# end
Device#
```

手順 4：設定の確認

```
Device # show running-config interface GigabitEthernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport access vlan 33
switchport mode access
Switch#
```

手順 5：インターフェイス スイッチポートの確認

```
Device # show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 33 (test)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: None
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

関連トピック

switchport mode, （477 ページ）

switchport mode

ポートのVLANメンバーシップ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 **switchport mode** コマンドを使用します。モードをデバイスに適したデフォルト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**| **dynamic** | {**auto**| **desirable**}| **trunk**}

noswitchport mode {**access**| **dynamic** | {**auto**| **desirable**}| **trunk**}

構文の説明

access	ポートをアクセス モードに設定します（**switchport access vlan** インターフェイス コンフィギュレーション コマンドの設定に応じて、スタティック アクセスまたはダイナミック アクセスのいずれか）。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。
dynamic auto	ポート トランキング モードのダイナミック パラメータを auto に設定して、インターフェイスがリンクをトランク リンクに変換するように指定します。これがデフォルトのスイッチポート モードになります。
dynamic desirable	ポート トランキング モードのダイナミック パラメータを desirable に設定して、インターフェイスがリンクをトランク リンクにアクティブに変換するように指定します。
trunk	ポートを無条件にトランクに設定します。ポートはトランキング VLAN レイヤ 2インターフェイスです。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 デバイス 間、または デバイス とルータ間のポイントツーポイント リンクです。

コマンド デフォルト

デフォルト モードは **dynamic auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

（注） **dot1q-tunnel** キーワードは CLI に表示されますが、サポートされていません。

access 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のみです。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、隣接インターフェイスがリンクから非トランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

trunk モードを開始すると、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 モードを開始すると、隣接インターフェイスが **trunk** または **desirable** モードに設定された場合に、インターフェイスはリンクをトランク リンクに変換します。

dynamic desirable モードを開始すると、隣接インターフェイスが **trunk**、**desirable**、または **auto** モードに設定された場合に、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 Dynamic Trunking Protocol（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。この問題を避けるには、DTP をサポートし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、DTP をオフにします。

- 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へ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。

アクセス ポートとトランク ポートは、互い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。

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* 行と *Operational Mode* 行の情報を調べます。

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。

```
Device(config)# interface gigabitethernet2/0/1
Device(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。

```
Device(config)# interface gigabitethernet2/0/1
Device(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。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode trunk
```

関連トピック

switchport access vlan, （475 ページ）

switchport nonegotiate

Dynamic Trunking Protocol（DTP）ネゴシエーション パケットがレイヤ 2 インターフェイス上で送信されない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 **switchport nonegotiate** コマンドを使用します。デフォルト設定に戻すには、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。

コマンド 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

no switchport nonegotiate コマンドは nonegotiate ステータスを解除します。

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上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。

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。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport nonegotiate
```

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

関連トピック

switchport mode, （477 ページ）

switchport voice vlan

ポートに音声 VLAN 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 **switchport voice 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。

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged** | **name***vlan_name*}

no switchport voice vlan

構文の説明

vlan-id	音声トラフィックに使用するVLAN。指定できる範囲は1～4094です。デフォルトでは、Cisco IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。
dot1p	IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話機を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。
none	音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。
untagged	タグなしの音声トラフィックを送信するようにIP Phoneを設定します。これがIP Phone のデフォルト設定になります。
name*vlan_name*	（任意）音声トラフィックに使用する VLAN 名を指定します。最大 128 文字を入力できます。

コマンド デフォルト

デフォルトでは、IP Phone を自動設定しません（**none**）。

デフォルトでは、IP Phone はフレームにタグを付けません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	音声 VLAN に VLAN 名を指定するオプション。「**name**」キーワー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。

デバイスの 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、Cisco IP Phoneに設定情報を送信する必要があります。デフォルトでは、CDP はインターフェイス上でグローバルにイネーブルです。

音声 VLAN をイネーブルにする前に、**trust device cisco-phone** インターフェイス コンフィギュレーション コマンドを入力してインターフェイス上でサービス品質（QoS）をイネーブルに設定しておくことを推奨します。Auto QoS 機能を使用すると、これらは自動的に設定されます。

VLAN ID を入力すると、IP Phone は IEEE 802.1Q フレームの音声トラフィックを指定された VLAN ID タグ付きで転送します。デバイスは IEEE 802.1Q 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、デバイス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 には、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。

この例では、最初に VLAN 名と VLAN ID を対応させることにより VLAN データベースを作成し、次にインターフェイスのアクセス モードで VLAN（名前を使用して）を設定する方法を示しています。設定を確認するには、特権 EXEC コマンドで **show interfaces***interface-id***switchport** を入力し、音声 VLAN の行の情報を調べます。

パート 1 - VLAN データベースに入力する

```
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

パート 2 - VLAN データベースを確認する

```
Device# show vlan id 55
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
55 test active
VLAN Type  SAID   MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ------ ---- ------ ------ -------- --- -------- ------ ------
55   enet  100055 1500 -      -      -        -   -        0      0
Remote SPAN VLAN
----------------
Disabled
Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
```

パート 3 - VLAN 名を使用して VLAN をインターフェイスに割り当てる

```
Device# configure terminal
Device(config)# interface gigabitethernet3/1/1
```

```
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan name test
Device(config-if)# end
Device#
```

パート 4 - 設定を確認する

```
Device# show running-config
interface gigabitethernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport voice vlan 55
switchport mode access
Switch#
```

パート 5 - インターフェイス スイッチポートでも確認できる

```
Device# show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Device#
```

関連トピック

show interfaces, （205 ページ）

switchport priority extend, （1430 ページ）

udld

単方向リンク検出（UDLD）で、アグレッシブモードまたは通常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、グローバル コンフィギュレーション モードで **udld** コマンドを使用します。すべての光ファイバ ポート上でアグレッシブ モード UDLD または通常モード UDLDをディセーブルにするには、このコマンドの **no** 形式を使用します。

udld {**aggressive**| **enable**| **message time** *message-timer-interval*}

no udld {**aggressive**| **enable**| **message**}

構文の説明

aggressive	すべての光ファイバ インターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。
enable	すべての光ファイバ インターフェイスにおいて、通常モードで UDLD をイネーブルにします。
message time *message-timer-interval*	アドバタイズメント フェーズにあり、双方向と判別されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。指定できる範囲は 1 ～ 90 秒です。デフォルトは 15 秒です。

コマンド デフォルト

すべてのインターフェイスで UDLD はディセーブルです。

メッセージ タイマーは 15 秒に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。通常モードおよびアグレッシブ モードについては、*Catalyst 2960-X Switch Layer 2 Configuration GuideCatalyst 2960-XR Switch Layer 2 Configuration GuideLayer 2/3 Configuration Guide (Catalyst 3850 Switches)*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 負荷との折り合いをつけることになります。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：グローバルに UDLD を再びイネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力：指定されたインターフェイスの UDLD を再びイネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド：自動的に UDLD error-disabled ステートから回復します。

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。

```
Device(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。

関連トピック

show udld, （470 ページ）
udld port, （486 ページ）
udld reset, （488 ページ）

udld port

個々のインターフェイスで単方向リンク検出（UDLD）をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぐには、インターフェース コンフィギュレーション モードで **udld port** コマンドを使用します。**udld** グローバル コンフィギュレーション コマンド設定に戻すか、または非光ファイバ 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、このコマンドの **no** 形式を使用します。

udld port [aggressive]

no udld port [aggressive]

構文の説明

aggressive	（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。

コマンド デフォルト

光ファイバ インターフェイスでは、UDLD はディセーブルになっていますが、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応じて UDLD をイネーブルにします。

非光ファイバ インターフェイスでは、UDLD はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

UDLD 対応ポートが別のデバイスの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。

UDLD を通常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 コマンドの設定を上書きする場合は、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：グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力：指定したインターフェイスで UDLD を再度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。

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。

```
Device(config)# interface gigabitethernet6/0/1
Device(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。

```
Device(config)# interface gigabitethernet6/0/1
Device(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。

関連トピック

show udld, （470 ページ）

udld, （484 ページ）

udld reset, （488 ページ）

udld reset

単方向リンク検出（UDLD）によりディセーブルにされたインターフェイスをすべてリセットし、インターフェイスのトラフィックを再開させるには、特権 EXEC モードで **udld reset** コマンドを使用します（イネーブルの場合には、スパニングツリー、Port Aggregation Protocol（PAgP）、Dynamic Trunking Protocol（DTP）などの他の機能を介することで有効になります）。

udld reset

構文の説明デフォルト

特権 EXEC モードには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

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。

```
Device# udld reset
1 ports shutdown by UDLD were reset.
```

関連トピック

show udld, （470 ページ）

udld, （484 ページ）

udld port, （486 ページ）

第 IX 部

Lightweight アクセス ポイント

- Cisco Lightweight アクセス ポイント コマンド，493 ページ

第 10 章

Cisco Lightweight アクセス ポイント コマンド

- ap auth-list ap-policy, 499 ページ
- ap bridging, 500 ページ
- ap capwap multicast, 501 ページ
- ap capwap retransmit, 502 ページ
- ap capwap timers, 503 ページ
- ap cdp, 505 ページ
- ap core-dump, 506 ページ
- ap country, 507 ページ
- ap crash-file, 508 ページ
- ap dot11 24ghz preamble, 509 ページ
- ap dot11 24ghz dot11g, 510 ページ
- ap dot11 5ghz channelswitch mode, 511 ページ
- ap dot11 5ghz power-constraint, 512 ページ
- ap dot11 beaconperiod, 513 ページ
- ap dot11 beamforming, 514 ページ
- ap dot11 cac media-stream, 515 ページ
- ap dot11 cac multimedia, 517 ページ
- ap dot11 cac video, 519 ページ
- ap dot11 cac voice, 520 ページ
- ap dot11 cleanair, 524 ページ

- ap dot11 cleanair alarm air-quality, 525 ページ
- ap dot11 cleanair alarm device, 525 ページ
- ap dot11 cleanair device, 527 ページ
- ap dot11 dot11n, 528 ページ
- ap dot11 dtpc, 531 ページ
- ap dot11 edca-parameters, 532 ページ
- ap dot11 rrm group-mode, 533 ページ
- ap dot11 rrm channel cleanair-event, 534 ページ
- ap dot11 l2roam rf-params, 535 ページ
- ap dot11 media-stream, 537 ページ
- ap dot11 rrm ccx location-measurement, 538 ページ
- ap dot11 rrm channel dca, 539 ページ
- ap dot11 rrm group-member, 541 ページ
- ap dot11 rrm logging, 542 ページ
- ap dot11 rrm monitor, 543 ページ
- ap dot11 rrm ndp-type, 544 ページ
- ap dot11 5ghz dot11ac frame-burst, 545 ページ
- ap dot1x max-sessions, 546 ページ
- ap dot1x username, 547 ページ
- ap ethernet duplex, 548 ページ
- ap group, 549 ページ
- ap image, 550 ページ
- ap ipv6 tcp adjust-mss, 551 ページ
- ap led, 552 ページ
- ap link-encryption, 553 ページ
- ap link-latency, 553 ページ
- ap mgmtuser username, 554 ページ
- ap name ap-groupname, 556 ページ
- ap name antenna band mode, 557 ページ
- ap name bhrate, 558 ページ
- ap name bridgegroupname, 558 ページ

- ap name bridging, 559 ページ
- ap name cdp interface, 560 ページ
- ap name console-redirect, 561 ページ
- ap name capwap retransmit, 562 ページ
- ap name command, 563 ページ
- ap name core-dump, 564 ページ
- ap name country, 565 ページ
- ap name crash-file, 566 ページ
- ap name dot11 24ghz rrm coverage, 567 ページ
- ap name dot11 49ghz rrm profile, 568 ページ
- ap name dot11 5ghz rrm channel, 570 ページ
- ap name dot11 antenna, 571 ページ
- ap name dot11 antenna extantgain, 572 ページ
- ap name dot11 cleanair, 573 ページ
- ap name dot11 dot11n antenna, 574 ページ
- ap name dot11 dual-band cleanair, 575 ページ
- ap name dot11 dual-band shutdown, 576 ページ
- ap name dot11 rrm ccx, 576 ページ
- ap name dot11 rrm profile, 577 ページ
- ap name dot11 txpower, 579 ページ
- ap name dot1x-user, 580 ページ
- ap name ethernet, 581 ページ
- ap name ethernet duplex, 582 ページ
- ap name key-zeroize, 584 ページ
- ap name image, 584 ページ
- ap name ipv6 tcp adjust-mss, 585 ページ
- ap name jumbo mtu, 586 ページ
- ap name lan, 587 ページ
- ap name led, 588 ページ
- ap name link-encryption, 588 ページ
- ap name link-latency, 589 ページ

- ap name location, 590 ページ
- ap name mgmtuser, 591 ページ
- ap name mode, 592 ページ
- ap name monitor-mode, 594 ページ
- ap name monitor-mode dot11b, 595 ページ
- ap name name, 596 ページ
- ap name no dot11 shutdown, 596 ページ
- ap name power, 597 ページ
- ap name shutdown, 598 ページ
- ap name slot shutdown, 599 ページ
- ap name sniff, 600 ページ
- ap name ssh, 601 ページ
- ap name telnet, 602 ページ
- ap name power injector, 603 ページ
- ap name power pre-standard, 604 ページ
- ap name reset-button, 604 ページ
- ap name reset, 605 ページ
- ap name slot, 606 ページ
- ap name static-ip, 607 ページ
- ap name stats-timer, 609 ページ
- ap name syslog host, 609 ページ
- ap name syslog level, 610 ページ
- ap name tcp-adjust-mss, 611 ページ
- ap name tftp-downgrade, 612 ページ
- ap power injector, 613 ページ
- ap power pre-standard, 614 ページ
- ap reporting-period, 615 ページ
- ap reset-button, 615 ページ
- service-policy type control subscriber, 616 ページ
- ap static-ip, 617 ページ
- ap syslog, 618 ページ

- ap name no controller , 619 ページ
- ap tcp-adjust-mss size, 620 ページ
- ap tftp-downgrade, 621 ページ
- config wireless wps rogue client mse, 622 ページ
- clear ap name tsm dot11 all, 623 ページ
- clear ap config, 624 ページ
- clear ap eventlog-all, 625 ページ
- clear ap join statistics, 625 ページ
- clear ap mac-address, 626 ページ
- clear ap name wlan statistics, 627 ページ
- debug ap mac-address, 628 ページ
- show ap cac voice, 628 ページ
- show ap capwap, 630 ページ
- show ap cdp, 631 ページ
- show ap config dot11, 632 ページ
- show ap config dot11 dual-band summary, 633 ページ
- show ap config fnf, 633 ページ
- show ap config, 634 ページ
- show ap crash-file, 635 ページ
- show ap data-plane, 635 ページ
- show ap dot11 l2roam, 636 ページ
- show ap dot11 cleanair air-quality, 637 ページ
- show ap dot11 cleanair config, 638 ページ
- show ap dot11 cleanair summary, 640 ページ
- show ap dot11, 640 ページ
- show ap env summary, 645 ページ
- show ap ethernet statistics, 646 ページ
- show ap gps-location summary, 646 ページ
- show ap groups, 647 ページ
- show ap groups extended, 648 ページ
- show ap image, 648 ページ

- show ap is-supported, 649 ページ
- show ap join stats summary, 650 ページ
- show ap link-encryption, 650 ページ
- show ap mac-address, 651 ページ
- show ap monitor-mode summary, 653 ページ
- show ap name auto-rf, 653 ページ
- show ap name bhmode, 655 ページ
- show ap name bhrate, 656 ページ
- show ap name cac voice, 657 ページ
- show ap name config fnf, 658 ページ
- show ap name dot11 call-control, 658 ページ
- show ap name cable-modem, 659 ページ
- show ap name capwap retransmit, 660 ページ
- show ap name ccx rm, 661 ページ
- show ap name cdp, 662 ページ
- show ap name channel, 662 ページ
- show ap name config, 663 ページ
- show ap name config dot11, 665 ページ
- show ap name config slot, 668 ページ
- show ap name core-dump, 671 ページ
- show ap name data-plane, 672 ページ
- show ap name dot11, 673 ページ
- show ap name dot11 cleanair, 676 ページ
- show ap name env, 677 ページ
- show ap name ethernet statistics, 677 ページ
- show ap name eventlog, 678 ページ
- show ap gps-location summary, 679 ページ
- show ap name image, 679 ページ
- show ap name inventory, 680 ページ
- show ap name lan port, 681 ページ
- show ap name link-encryption, 682 ページ

- show ap name service-policy, 683 ページ
- show ap name tcp-adjust-mss, 683 ページ
- show ap name wlan, 684 ページ
- show ap name wlandot11 service policy, 685 ページ
- show ap slots, 686 ページ
- show ap summary, 687 ページ
- show ap tcp-adjust-mss, 688 ページ
- show ap universal summary, 688 ページ
- show ap uptime, 689 ページ
- show wireless ap summary, 690 ページ
- show wireless client ap, 690 ページ
- test ap name, 691 ページ
- test capwap ap name, 692 ページ
- trapflags ap, 693 ページ
- wireless wps rogue ap rldp alarm-only, 694 ページ
- wireless wps rogue ap rldp auto-contain, 695 ページ

ap auth-list ap-policy

デバイス に参加しているすべての Cisco Lightweight アクセス ポイントの認可ポリシーを設定するには、**apauth-listap-policy** コマンドを使用します。デバイス に参加しているすべての Cisco Lightweight アクセス ポイントの認可ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

ap auth-list ap-policy {**authorize-ap**| **lsc**| **mic**| **ssc**}

no ap auth-list ap-policy {**authorize-ap**| **lsc**| **mic**| **ssc**}

構文の説明

authorize-ap	許可ポリシーを有効にします。
lsc	ローカルで有効な証明書を持つアクセス ポイントの接続を有効にします。
mic	製造元でインストールされる証明書を持つアクセス ポイントの接続を有効にします。
ssc	自己署名証明書を持つアクセス ポイントの接続を有効にします。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの許可ポリシーを有効にする例を示します。

```
Device(config)# ap auth-list ap-policy authorize-ap
```

次に、ローカルで有効な証明書を持つアクセス ポイントの接続を有効にする例を示します。

```
Device(config)# ap auth-list ap-policy lsc
```

次に、製造元でインストールされる証明書を持つアクセス ポイントの接続を有効にする例を示します。

```
Device(config)# ap auth-list ap-policy mic
```

次に、自己署名証明書を持つアクセス ポイントの接続を有効にする例を示します。

```
Device(config)# ap auth-list ap-policy ssc
```

ap bridging

Cisco Lightweight アクセス ポイントでイーサネットと 802.11 の間のブリッジングを有効にするには、**apbridging** コマンドを使用します。Cisco Lightweight アクセス ポイントでイーサネットと 802.11 の間のブリッジングを無効にするには、このコマンドの **no** 形式を使用します。

ap bridging

no ap bridging

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なしグローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、Lightweight アクセス ポイントでイーサネット間ブリッジングを有効にする例を示します。

```
Device(config)# ap bridging
```

次に、Lightweight アクセス ポイントでイーサネット間ブリッジングを無効にする例を示します。

```
Device(config)# no ap bridging
```

ap capwap multicast

マルチキャスト転送が有効のときにマルチキャスト トラフィックを受信するためにすべてのアクセス ポイントによって使用されるマルチキャスト アドレスを設定し、アクセス ポイントに送信されるマルチキャスト パケットの外部 Quality of Service（QoS）レベルを設定するには、**ap capwap multicast** コマンドを使用します。

ap capwap multicast {*multicast-ip-address*| **service-policy output** *pollicymap-name*}

構文の説明

multicast-ip-address	マルチキャスト IP アドレス。
service-policy	マルチキャスト アクセス ポイントのトンネル QoS ポリシーを指定します。
output	ポリシー マップ名を出力に割り当てます。
policymap-name	サービス ポリシー マップ名。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、マルチキャスト転送が有効のときにマルチキャスト トラフィックを受信するためにすべてのアクセス ポイントによって使用されるマルチキャスト アドレスを設定する例を示します。

```
Device(config)# ap capwap multicast 239.2.2.2
```

次に、マルチキャスト アクセス ポイントのトンネル マルチキャスト QoS サービス ポリシーを設定する例を示します。

```
Device(config)# ap capwap multicast service-policy output tunnmulpolicy
```

ap capwap retransmit

Control And Provisioning of Wireless Access Points（CAPWAP）制御パケットの再送信回数と制御パケットの再送信間隔を設定するには、**ap capwap retransmit** コマンドを使用します。

ap capwap retransmit {**count** *retransmit-count*| **interval** *retransmit-interval*}

構文の説明

count *retransmit-count*	アクセスポイントのCAPWAP制御パケットの再送信回数を指定します。 （注） 回数は 3 ～ 8 です。
interval *retransmit-interval*	アクセスポイントのCAPWAP制御パケットの再送信間隔を指定します。 （注） 間隔は 2 ～ 5 秒です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの CAPWAP 制御パケットの再送信回数を設定する例を示します。

```
Device# ap capwap retransmit count 3
```

次に、アクセス ポイントの CAPWAP 制御パケットの再送信間隔を設定する例を示します。

```
Device# ap capwap retransmit interval 5
```

ap capwap timers

高度なタイマー設定を指定するには、**apcapwaptimers** コマンドを使用します。

ap capwap timers {**discovery-timeout** *seconds*| **fast-heartbeat-timeout local** *seconds*| **heartbeat-timeout** *seconds*| **primary-discovery-timeout** *seconds*| **primed-join-timeout** *seconds*}

構文の説明

discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウトを指定します。 （注） Cisco Lightweight アクセス ポイントの検出タイムアウトは、アクセス ポイントが応答しなかったとみなす前にシスコのデバイスが応答のないアクセス ポイントの応答を待つ時間です。
seconds	Cisco Lightweight アクセス ポイントの検出タイムアウト（1 ～ 10 秒）。 （注） デフォルトは 10 秒です。
fast-heartbeat-timeoutlocal	ローカル アクセス ポイントまたはすべてのアクセス ポイントのデバイス障害を検出するために要する時間を短縮する高速ハートビート タイマーを有効にします。
seconds	デバイス障害を検出するために要する時間を短縮する小さい値のハートビート間隔（1～10 秒）。 （注） デフォルトでは高速ハートビート タイムアウト間隔が無効になっています。

heartbeat-timeout	Cisco Lightweight アクセス ポイントのハートビート タイムアウトを指定します。 （注） Cisco Lightweight アクセス ポイントのハートビート タイムアウトは、Cisco Lightweight アクセス ポイントがシスコのデバイスにハートビート キープアライブ信号を送信する頻度を制御します。 この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。
seconds	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値（1 ～ 30 秒）。 （注） デフォルトは 30 秒です。
primary-discovery-timeout	アクセス ポイントのプライマリ ディスカバリ要求タイマーを指定します。このタイマーは、設定されているプライマリ、セカンダリ、またはターシャリ デバイスを検出するためにアクセス ポイントが取る時間を決定します。
seconds	アクセス ポイントのプライマリ検出要求タイマー（30 ～ 3600 秒）。 （注） デフォルトは 120 秒です。
primed-join-timeout	認証タイムアウトを指定します。プライマリ デバイスが応答不能になったと判断するためにアクセス ポイントが取る時間を決定します。アクセス ポイントは、デバイスへの接続が復元されるまで、デバイスへの参加を試みなくなります。
seconds	認証応答タイムアウト（120 ～ 43200 秒）。 （注） デフォルトは 120 秒です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、タイムアウト値を 7 でアクセス ポイント検出タイムアウトを設定する例を示します。

```
Device(config)# ap capwap timers discovery-timeout 7
```

次に、すべてのアクセスポイントを対象にファーストハートビート間隔を有効にする例を示します。

```
Device(config)# ap capwap timers fast-heartbeat-timeout 6
```

次に、アクセス ポイントのハートビート タイムアウトを 20 に設定する例を示します。

```
Device(config)# ap capwap timers heartbeat-timeout 20
```

次に、アクセス ポイントのプライマリ検出要求タイマーを 1200 秒に設定する例を示します。

```
Device(config)# ap capwap timers primary-discovery-timeout 1200
```

次に、認証タイムアウトを 360 秒に設定する例を示します。

```
Device(config)# ap capwap timers primed-join-timeout 360
```

ap cdp

Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を有効にするには、**apcdp** コマンドを使用します。Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を無効にするには、このコマンドの **no** 形式を使用します。

ap cdp [**interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}]

no ap cdp [**interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}]

構文の説明

interface	（任意）特定のインターフェイスの CDP を指定します。
ethernet	イーサネット インターフェイスの CDP を指定します。
ethernet-id	イーサネット インターフェイス番号（0 ～ 3）。
radio	無線インターフェイスの CDP を指定します。
radio-id	無線番号（0 ～ 3）。

コマンド デフォルト

すべてのアクセス ポイントで無効になっています。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

no apcdp コマンドは、デバイスに参加しているすべてのアクセス ポイントおよび今後参加するすべてのアクセス ポイントの CDP を無効にします。CDP は、デバイスまたはアクセス ポイントのリブート後も現在と将来のアクセス ポイントで無効のままになります。CDP を有効にするには、**apcdp** コマンドを入力します。

（注） イーサネット/無線インターフェイス上の CDP は、CDP が有効になっている場合にだけ使用できます。デバイスに参加しているすべてのアクセス ポイントで CDP を有効にした後は、**ap name** *Cisco-AP* **cdp** コマンドを使用して、個々のアクセス ポイントで CDP を無効にし、再度有効にすることができます。デバイスに参加しているすべてのアクセス ポイントで CDP を無効にした後は、個々のアクセス ポイントで CDP を有効にし、その後、無効にすることができます。

次に、すべてのアクセス ポイントで CDP を有効にする例を示します。

```
Device(config)# ap cdp
```

次に、すべてのアクセス ポイントでイーサネット インターフェイス番号 0 の CDP を有効にする例を示します。

```
Device(config)# ap cdp ethernet 0
```

ap core-dump

Cisco Lightweight アクセス ポイントのメモリ コア ダンプ設定を有効にするには、**apcore-dump** コマンドを使用します。Cisco Lightweight アクセス ポイントのメモリ コア ダンプ設定を無効にするには、このコマンドの **no** 形式を使用します。

ap core-dump *tftp-ip-addr filename* {**compress| uncompress**}

no ap core-dump

構文の説明

tftp-ip-addr	アクセス ポイントがコア ダンプ ファイルを送信する Trivial File Transfer Protocol（TFTP）サーバの IP アドレス。

filename	コア ファイルのラベルを付けるためにアクセス ポイントが使用する名前。
compress	コア ダンプ ファイルを圧縮します。
uncompress	コア ダンプ ファイルを圧縮解除します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

アクセス ポイントは TFTP サーバに到達できる必要があります。

次に、コア ダンプ ファイルを設定して圧縮する例を示します。

```
Device(config)# ap core-dump 192.0.2.51 log compress
```

ap country

デバイスの 1 つ以上の国コードを設定するには、**apcountry** コマンドを使用します。

ap country *country-code*

構文の説明

country-code	1 つ以上（複数の場合はカンマ区切り）の 2 文字または 3 文字の国番号。

コマンド デフォルト

US（米国）の国コード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

Cisco デバイス は、ネットワーク管理者または資格のある IP プロフェッショナルがインストールしてください。その際、正しい国コードを選択する必要があります。インストール後は、法的な規制基準を遵守するためおよび、適切なユニット機能を保証するために、ユニットへのアクセスはパスワードで保護する必要があります。最新の国コードおよび規制区域については、関連する製品マニュアルを参照してください。

次に、デバイスで国コードを IN（インド）および FR（フランス）に設定する例を示します。

```
Device(config)# ap country IN,FR
```

ap crash-file

クラッシュおよび無線コア ダンプ ファイルを削除するには、**apcrash-file** コマンドを使用します。

ap crash-file {**clear-all**| **delete** *filename*}

構文の説明

clear-all	クラッシュおよび無線コア ダンプ ファイルを削除します。
delete	単一のクラッシュおよび無線コア ダンプ ファイルを削除します。
filename	削除するファイルの名前を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのクラッシュ ファイルを削除する例を示します。

```
Device# ap crash-file clear-all
```

次に、クラッシュ ファイル 1 を削除する例を示します。

```
Device# ap crash-file delete crash-file-1
```

ap dot11 24ghz preamble

サブクローズ 17.2.2.2 で定義されている短いプリアンブルだけを有効にするには、**apdot1124ghzpreamble** コマンドを使用します。長いプリアンブル（802.11b 以前のデバイスとの下位互換性のため、これらのデバイスが依然としてネットワーク上にある場合）または短いプリアンブル（従来の802.11b以前のデバイスがネットワークに存在しない場合の推奨）を有効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz preamble short

no ap dot11 24ghz preamble short

構文の説明

short	短い 802.11b プリアンブルを指定します。

コマンド デフォルト

短いプリアンブル

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

（注） **apdot1124ghzpreamble** コマンドを使用するには、**Save** コマンドで Cisco デバイスをリブート（システムをリセット）する必要があります。

このパラメータは、SpectraLink NetLink 電話など一部のレガシー クライアントのためにこの Cisco デバイスを最適化するために、long に設定する必要があることがあります。

このコマンドは、CLI インターフェイスがアクティブなときはいつでも使用できます。

次に、長いプリアンブルと短いプリアンブルの両方を有効にする例を示します。

```
Device(config)# no ap dot11 24ghz preamble short
```

ap dot11 24ghz dot11g

シスコ ワイヤレス LAN ソリューション 802.11g ネットワークを有効にするには、**apdot1124ghzdot11g** コマンドを使用します。シスコ ワイヤレス LAN ソリューション 802.11g ネットワークを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz dot11g

no ap dot11 24ghz dot11g

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

apdot1124ghzdot11g コマンドを入力する前に、**apdot1124ghzshutdown** コマンドを使用して 802.11 シスコ無線を無効にしてください。

802.11g ネットワークのサポートを設定した後、**noapdot1124ghzshutdown** コマンドを使用して 802.11 2.4 Ghz 無線を有効にしてください。

次に、802.11g ネットワークを有効にする例を示します。

```
Device(config)# ap dot11 24ghz dot11g
```

ap dot11 5ghz channelswitch mode

802.11h チャネル スイッチ アナウンスを設定するには、**apdot115ghzchannelswitchmode** コマンドを使用します。802.11h チャネル スイッチ アナウンスを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz channelswitch mode *value*

no ap dot11 5ghz channelswitch mode

構文の説明

value	802.11h チャネル スイッチ通知の値。 （注） 次の 2 つの値のどちらでも指定できます。 • 0：チャネル スイッチ アナウンスが無効であることを示します。 • 1：チャネル スイッチ アナウンスが有効であることを示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、802.11h スイッチ アナウンスを無効にする例を示します。

```
Device(config)# ap dot11 5ghz channelswitch mode 1
```

ap dot11 5ghz power-constraint

802.11h の電力制限値を設定するには、**apdot115ghzpower-constraint** コマンドを使用します。802.11h の電力制限値を削除するには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz power-constraint *value*

no ap dot11 5ghz power-constraint

構文の説明

value	802.11h の電力制限値。 （注） 範囲は、0 ～ 30 dBm です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、802.11h 電力制限を 5 dBm に設定する例を示します。

```
Device(config)# ap dot11 5ghz power-constraint 5
```

ap dot11 beaconperiod

2.4 GHz 帯域または 5 GHz 帯域のビーコン周期をグローバルに変更するには、**apdot11beaconperiod** コマンドを使用します。

（注） このコマンドを使用する前に、802.11 ネットワークを無効にします。「使用上のガイドライン」の項を参照してください。

ap dot11 {**24ghz**| **5ghz**} **beaconperiod** *time*

構文の説明

24ghz	2.4 GHz 帯域の設定を指定します。
5ghz	5 GHz 帯域の設定を指定します。
beaconperiod	ネットワークのビーコンをグローバルに指定します。
time	時間単位（TU）でのビーコン間隔。1 TU は 1024 マイクロ秒です。範囲は 20 ～ 1000 です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

Cisco ワイヤレス LAN 802.11 ネットワークでは、すべての Cisco Lightweight アクセス ポイント（無線 LAN）が定期的にビーコンをブロードキャストします。このビーコンは、クライアントに

ワイヤレス サービスが使用可能なことを通知し、クライアントは Lightweight アクセス ポイントと同期できます。

ビーコン周期を変更する前に、**apdot11 {24ghz | 5ghz} shutdown** コマンドを使用して 802.11 ネットワークを無効にしていることを確認してください。ビーコン周期を変更した後に、**noapdot11 {24ghz | 5ghz} shutdown** コマンドを使用して 802.11 ネットワークを有効にしてください。

次に、120 時間単位のビーコン周期に合わせて 5 GHz 帯域を設定する例を示します。

```
Device(config)# ap dot11 5ghz beaconperiod 120
```

ap dot11 beamforming

ネットワークまたは個別の無線に対してビームフォーミングを有効にするには、**apdot11beamforming** コマンドを使用します。

ap dot11 {24ghz| 5ghz} beamforming

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
beamforming	ネットワークに対してビームフォーミングを指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

ネットワークに対してビームフォーミングを有効にすると、そのネットワーク タイプに対応するすべての無線に対してビームフォーミングが自動的に有効になります。

ビームフォーミングを使用する際は、次のガイドラインに従ってください。

- ビームフォーミングは、レガシー直交周波数分割多重（OFDM）データ レート（6、9、12、18、24、36、48、および 54 Mbps）でサポートされています。

（注） ビームフォーミングは、直接拡散方式のデータ レート（1 および 2 Mbps）および相補コード キー（CCK）のデータ レート（5.5 および 11 Mbps）ではサポートされません。

- ビームフォーミングは、802.11n に対応したアクセス ポイント（AP1260、AP3500、および AP3600）でだけサポートされます。
- 送信用に 2 本以上のアンテナを有効にする必要があります。
- 受信用に 3 本すべてのアンテナを有効にする必要があります。
- OFDM レートを有効にする必要があります。

  送信アンテナがアンテナ設定により 1 本に制限されている場合、あるいは OFDM レートが無効になっている場合、ビームフォーミングは使用されません。

次に、5 GHz 帯域に対してビームフォーミングを有効にする例を示します。

```
Device(config)# ap dot11 5ghz beamforming
```

ap dot11 cac media-stream

2.4 GHz 帯域と 5 GHz 帯域のメディア ストリームのコール アドミッション制御（CAC）の音声およびビデオ品質パラメータを設定するには、**apdot11cacmedia-stream** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **cac media-stream multicast-direct** {**max-retry-percent** *retryPercent*| **min-client-rate**{**eighteen**| **eleven**| **fiftyFour**| **fivePointFive**| **fortyEight**| **nine**| **oneFifty**| **oneFortyFourPointFour**| **oneThirty**| **oneThirtyFive**| **seventyTwoPointTwo**| **six**| **sixtyFive**| **thirtySix**| **threeHundred**| **twelve**| **twentyFour**| **two**| **twoSeventy**}}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
multicast-direct	マルチキャスト直接メディア ストリーム用の CAC パラメータを指定します。
max-retry-percent	マルチキャスト直接メディア ストリームに許可される最大再試行回数の割合を指定します。

retryPercent	マルチキャスト直接メディア ストリームに許可される最大再試行回数の割合。 （注） 範囲は 0 ～ 100 です。
min-client-rate	マルチキャスト直接メディア ストリーム用にクライアントへの最小データ伝送レートを指定します（マルチキャスト直接ユニキャスト ストリームを受信するためにクライアントが送信する必要があるレート）。 伝送レートがこのレートを下回ると、ビデオが起動しないか、クライアントが不良クライアントとして分類される可能性があります。不良クライアント ビデオは、より良いエフォートの QoS のために降格されたり、拒否される可能性があります。
min-client-rate	次のレートを選択できます。 • **eighteen** • **eleven** • **fiftyFour** • **fivePointFive** • **fortyEight** • **nine** • **one** • **oneFifty** • **oneFortyFourPointFour** • **oneThirty** • **oneThirtyFive** • **seventyTwoPointTwo** • **six** • **sixtyFive** • **thirtySix** • **threeHundred** • **twelve** • **twentyFour** • **two** • **twoSeventy**

コマンド デフォルト

最大再試行回数の割合のデフォルト値は 80 です。80 を超えると、ビデオが開始されないか、クライアントが不良クライアントとして分類される場合があります。不良クライアント ビデオは、より良いエフォートの QoS のために降格されたり、拒否されたりします。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **wlan***wlan_name***shutdown** コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **apdot11** {**24ghz** | **5ghz**} **shutdown** コマンドを入力して、設定する無線ネットワークを無効にします。
- 新しい設定を保存します。
- **apdot11** {**24ghz** | **5ghz**} **cacvoiceacm** コマンドまたは **apdot11** {**24ghz** | **5ghz**} **cacvideoacm** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、802.11a ネットワークの 90 としてマルチキャスト直接メディア ストリームの最大試行回数の割合を設定する例を示します。

```
Device(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

ap dot11 cac multimedia

2.4 GHz 帯域と 5 GHz 帯域のマルチメディアのコール アドミッション制御（CAC）の音声およびビデオ品質パラメータを設定するには、**apdot11cacmultimedia** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **cac multimedia max-bandwidth** *bandwidth*

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
max-bandwidth	2.4 GHz 帯域または 5 GHz 帯域で音声およびビデオ アプリケーション用に Wi-Fi Multimedia（WMM）クライアントに割り当てられる最大帯域幅の割合を指定します。
bandwidth	802.11a または 802.11b/g ネットワークで音声およびビデオ アプリケーション用に WMM クライアントに割り当てられる最大帯域幅の割合。クライアントが指定値に達すると、アクセスポイントはこの無線帯域での新しいマルチメディア フローを拒否します。範囲は 5 ～ 85% です。

コマンド デフォルト

デフォルト値は 75 % です

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **wlan***wlan_name***shutdown** コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **apdot11** {**24ghz** | **5ghz**} **shutdown** コマンドを入力して、設定する無線ネットワークを無効にします。

- 新しい設定を保存します。
- **apdot11** {**24ghz** | **5ghz**} **cacvoiceacm** コマンドまたは **apdot11** {**24ghz** | **5ghz**} **cacvideoacm** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、5 GHz 帯域で音声およびビデオ アプリケーション用に WMM クライアントに割り当てられる最大帯域幅の割合を設定する例を示します。

```
Device(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

ap dot11 cac video

ビデオ カテゴリのコールアドミッション制御（CAC）パラメータを設定するには、**apdot11cacvideo** コマンドを使用します。ビデオ カテゴリの CAC パラメータを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**} **cac video** {**acm**| **max-bandwidth** *value*| **roam-bandwidth** *value*}

no ap dot11 {**24ghz**| **5ghz**} **cac video** {**acm**| **max-bandwidth** *value*| **roam-bandwidth** *value*}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
acm	2.4 GHz 帯域または 5 GHz 帯域の帯域幅ベースのビデオ CAC を有効にします。 （注） 2.4 GHz 帯域または 5 GHz 帯域の帯域幅ベースのビデオ CAC を無効にするには、**noapdot11** {**24ghz**	**5ghz**} **cacvideoacm** コマンドを使用します。
max-bandwidth	2.4 GHz 帯域または 5 GHz 帯域でビデオ アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。
value	5 ～ 85 % の帯域の割合値。
roam-bandwidth	2.4 GHz 帯域または 5 GHz 帯域での CAC の最大割り当て帯域幅のうち、ビデオ クライアントのローミング用に予約する割合を設定します。
value	0 ～ 85 % の帯域の割合値。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **wlan***wlan_name***shutdown** コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **apdot11 {24ghz | 5ghz} shutdown** コマンドを入力して、設定する無線ネットワークを無効にします。
- 新しい設定を保存します。
- **apdot11 {24ghz | 5ghz} cacvoiceacm** コマンドまたは **apdot11 {24ghz | 5ghz} cacvideoacm** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、帯域幅ベースの CAC をイネーブルにする例を示します。

```
Device(config)# ap dot11 24ghz cac video acm
```

次に、選択した無線帯域でビデオ アプリケーションに割り当てられる最大帯域幅の割合を指定する例を示します。

```
Device(config)# ap dot11 24ghz cac video max-bandwidth 50
```

次に、選択した無線帯域でビデオ クライアントのローミング用に予約された最大割り当て帯域幅の割合を指定する例を示します。

```
Device(config)# ap dot11 24ghz cac video roam-bandwidth 10
```

ap dot11 cac voice

音声カテゴリのコール アドミッション制御（CAC）パラメータを設定するには、**apdot11cacvoice** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **cac voice**{**acm**| **load-based**| **max-bandwidth** *value*| **roam-bandwidth** *value*| **sip** [**bandwidth** *bw*] **sample-interval** *value*| **stream-size** *x* **max-streams** *y*| **tspec-inactivity-timeout**{**enable**| **ignore**}}

構文の説明

24ghz	2.4 GHz 帯域を指定します。

5ghz	5 GHz 帯域を指定します。
acm	2.4 GHz 帯域または 5 GHz 帯域の帯域幅ベースの音声 CAC を有効にします。 （注） 2.4 GHz 帯域または 5 GHz 帯域の帯域幅ベースの音声 CAC を無効にするには、**noapdot11** {**24ghz** | **5ghz**} **cacvoiceacm** コマンドを使用します。
load-based	音声アクセス カテゴリで負荷ベースの CAC を有効にします。 （注） 2.4 GHz 帯域または 5 GHz 帯域の音声アクセス カテゴリで負荷ベースの CAC を無効にするには、**noapdot11** {**24ghz** | **5ghz**} **cacvoiceload-based** コマンドを使用します。
max-bandwidth	2.4 GHz 帯域または 5 GHz 帯域で音声アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。
value	5 ～ 85 % の帯域の割合値。
roam-bandwidth	2.4 GHz 帯域または 5 GHz 帯域での CAC の最大割り当て帯域幅のうち、音声クライアントのローミング用に予約する割合を設定します。
value	0 ～ 85 % の帯域の割合値。
sip	CAC のコーデック名とサンプル間隔をパラメータとして指定し、802.11 ネットワークのコールごとに必要な帯域幅を計算します。
bandwidth	（任意）SIP ベースのコールの帯域幅を指定します。
bw	帯域幅（kbps 単位）。次の帯域幅値は SIP コーデックのパラメータを指定します。 • 64kbps：SIP G711 コーデックに CAC パラメータを指定します。 • 8kbps：SIP G729 コーデックに CAC パラメータを指定します。 （注） デフォルト値は 64 Kbps です。

sample-interval	SIP コーデックのパケット化間隔を指定します。
value	ミリ秒単位のパケット化間隔。SIP コーデック値のサンプリング間隔は 20 秒です。
stream-size	2.4 GHz 帯域または 5 GHz 帯域で指定したデータレートでの集約音声 Wi-Fi マルチメディア（WMM）トラフィック仕様（TSPEC）ストリームの数を指定します。
x	ストリームのサイズ。ストリーム サイズの範囲は 84000 ～ 92100 です。
max-streams	TSPEC ごとのストリームの最大数を指定します。
y	音声ストリームの数（1 ～ 5）。 （注） デフォルトのストリーム数は 2 で、ストリームの平均データ レートは 84 Kbps です。
tspec-inactivity-timeout	TSPEC 非アクティブ タイムアウトの処理モードを指定します。 （注） アクセス ポイントから受信した Wi-Fi マルチメディア（WMM）トラフィック仕様（TSPEC）非アクティブ タイムアウトを処理または無視するには、このキーワードを使用します。非アクティブ タイムアウトが無視された場合、アクセス ポイントがそのクライアントの非アクティブ タイムアウトを報告しても、クライアント TSPEC は削除されません。
enable	TSPEC 無活動タイムアウト メッセージを処理します。
ignore	TSPEC 無活動タイムアウト メッセージを無視します。 （注） デフォルトは **ignore**（無効）です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **wlan***wlan_name***shutdown** コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **apdot11** {**24ghz | 5ghz**} **shutdown** コマンドを入力して、設定する無線ネットワークを無効にします。
- 新しい設定を保存します。
- **apdot11** {**24ghz | 5ghz**} **cacvoiceacm** コマンドまたは **apdot11** {**24ghz | 5ghz**} **cacvideoacm** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、帯域幅ベースの CAC をイネーブルにする例を示します。

```
Device(config)# ap dot11 24ghz cac voice acm
```

次に、音声アクセス カテゴリの負荷ベースの CAC を有効にする例を示します。

```
Device(config)# ap dot11 24ghz cac voice load-based
```

次に、選択した無線帯域で音声アプリケーション用に割り当てられる最大帯域幅の割合を指定する例を示します。

```
Device(config)# ap dot11 24ghz cac voice max-bandwidth 50
```

次に、選択した無線帯域で音声クライアントのローミング用に予約された最大割り当て帯域幅の割合を指定する例を示します。

```
Device(config)# ap dot11 24ghz cac voice roam-bandwidth 10
```

次に、2.4 GHz 帯域の G729 SIP コーデックの帯域幅と音声パケット化間隔を設定する例を示します。

```
Device(config)# ap dot11 24ghz cac voice sip bandwidth 8 sample-interval 40
```

次に、85000 のストリーム サイズと最大 5 ストリームで集約音声トラフィック仕様のストリームの数を設定する例を示します。

```
Device(config)# ap dot11 24ghz cac voice stream-size 85000 max-streams 5
```

次に、アクセス ポイントから受信した音声 TSPEC 非アクティブ タイムアウト メッセージをイネーブルにする方法を示します。

```
Device(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```

ap dot11 cleanair

802.11 ネットワークの CleanAir を設定するには、**apdot11cleanair** コマンドを使用します。802.11 ネットワークの CleanAir を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**} **cleanair**

no ap dot11 {**24ghz**| **5ghz**} **cleanair**

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
cleanair	2.4 GHz 帯域または 5 GHz 帯域の CleanAir を指定します。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz 帯域の CleanAir 設定を有効にする例を示します。

```
Device(config)# ap dot11 24ghz cleanair
```

ap dot11 cleanair alarm air-quality

Cisco Lightweight アクセス ポイントの CleanAir 電波品質アラームを設定するには、**apdot11cleanairalarmair-quality** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **cleanair alarm air-quality** [**threshold** *value*]

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
threshold	電波品質アラームのしきい値を指定します。
value	電波品質のアラームしきい値（1 = 電波品質が悪い、100 = 電波品質がよい）。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz のCleanAir 電波品質しきい値を 90 に設定する例を示します。

```
Device(config)# ap dot11 24ghz cleanair air-quality threshold 90
```

ap dot11 cleanair alarm device

2.4 GHz 帯域または 5 GHz 帯域で CleanAir 干渉デバイスのアラームを設定するには、**apdot11cleanairalarmdevice** コマンドを使用します。802.11 ネットワークで CleanAir 干渉デバイスのアラームを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**} **cleanair alarm device**{**all**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fh**| **inv**| **jammer**| **mw-oven**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**}

no ap dot11 {**24ghz**| **5ghz**} **cleanair**

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
all	すべてのデバイス タイプを一度に指定します。
bt-discovery	ディスカバリ モードの Bluetooth デバイスを指定します。
bt-link	Bluetooth アクティブ リンクを指定します。
canopy	Canopy デバイスを指定します。
cont-tx	連続トランスミッタを指定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話を指定します。
fh	周波数ホッピング デバイスを指定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスを指定します。
jammer	電波妨害装置を指定します。
mw-oven	電子レンジのデバイスを指定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスを指定します。
superag	802.11 SuperAG デバイスを指定します。
tdd-tx	TDD トランスミッタを指定します。
video	ビデオ カメラを指定します。
wimax-fixed	WiMax 固定デバイスを指定します。
wimax-mobile	WiMax モバイル デバイスを指定します。
xbox	Xbox デバイスを指定します。
zigbee	ZigBee デバイスを指定します。

コマンド デフォルト

デフォルト 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ZigBee 干渉検出のアラームを無効にする例を示します。

```
Device(config)# no ap dot11 24ghz cleanair alarm device zigbee
```

次に、Bluetooth リンク検出アラームを有効にする例を示します。

```
Device(config)# ap dot11 24ghz cleanair alarm device bt-link
```

ap dot11 cleanair device

CleanAir 干渉デバイスのタイプを設定するには、**apdot11cleanairdevice** コマンドを使用します。

ap dot11 24ghz cleanair device [**all**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fh**| **inv**| **jammer**| **mw-oven**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**]

構文の説明

all	すべてのデバイス タイプを指定します。
device	CleanAir 干渉デバイスのタイプを指定します。
bt-discovery	ディスカバリ モードの Bluetooth デバイスを指定します。
bt-link	Bluetooth アクティブ リンクを指定します。
canopy	Canopy デバイスを指定します。
cont-tx	連続トランスミッタを指定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタルコードレス電話を指定します。
fh	802.11 の周波数ホッピング デバイスを指定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスを指定します。
jammer	電波妨害装置を指定します。

mw-oven	電子レンジのデバイスを指定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスを指定します。
superag	802.11 SuperAG デバイスを指定します。
tdd-tx	TDD トランスミッタを指定します。
video	ビデオ カメラを指定します。
wimax-fixed	WiMax 固定デバイスを指定します。
wimax-mobile	WiMax モバイル デバイスを指定します。
xbox	Xbox デバイスを指定します。
zigbee	ZigBee デバイスを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ZigBee の干渉をモニタするようにデバイスを設定する例を示します。

```
Device(config)# ap dot11 24ghz cleanair device zigbee
```

ap dot11 dot11n

802.11n ネットワークを設定するには、**apdot11dot11n** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **dot11n** {**a-mpdu tx priority**{*priority_value* **all**}| **scheduler timeout rt***scheduler_value*}| **a-msdu tx priority**{*priority_value*| **all**}| **guard-interval** {**any**| **long**}| **mcs tx** *rate*| **rifs rx**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。

5ghz	5 GHz 帯域を指定します。
dot11n	802.11n サポートを有効にします。
a-mpdutxpriority	Aggregated MAC Protocol Data Unit（A-MPDU）伝送を使用する優先度レベルに関連するトラフィックを指定します。
priority_value	Aggregated MAC Protocol Data Unit（A-MPDU）の優先度レベル（0 ～ 7）。
all	すべての優先度レベルを一度に指定します。
a-msdutxpriority	Aggregated MAC Service Data Unit（A-MSDU）伝送を使用する優先度レベルに関連するトラフィックを指定します。
priority_value	Aggregated MAC Protocol Data Unit（A-MPDU）の優先度レベル（0 ～ 7）。
all	すべての優先度レベルを一度に指定します。
scheduler timeout rt	802.11n A-MPDU 伝送集約スケジューラのタイムアウト値（ミリ秒単位）を設定します。
scheduler_value	802.11n A-MPDU 伝送集約スケジューラのタイムアウト値（1 ～ 10000ミリ秒）。
guard-interval	ガード間隔を指定します。
any	短期または長期ガード間隔をイネーブルにします。
long	長期ガード間隔のみをイネーブルにします。
mcstx*rate*	データをアクセスポイントとクライアント間で送信できる変調および符号化方式（MCS）レートを指定します。
rate	変調および符号化方式のデータ レートを指定します。 （注） 範囲は 0 ～ 23 です。
rifsrx	データ フレーム間の Reduced Interframe Space（RIFS）を指定します。

コマンド デフォルト

デフォルトでは優先度 0 が有効になっています。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	scheduler、timeout、rt の各キーワードが追加されました。

使用上のガイドライン

集約は、パケットデータ フレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約には、次の 2 つの方法があります。

- A-MPDU：この集約はソフトウェアで実行されます。
- A-MSDU：この集約はハードウェアで実行されます。

トラフィック タイプごとに割り当てられた集約 MAC プロトコル データ ユニットの優先度は次のとおりです。

- 0：ベスト エフォート
- 1：バックグラウンド
- 2：スペア
- 3：エクセレント エフォート
- 4：制御ロード
- 5：ビデオ（100 ms 未満の遅延およびジッタ）
- 6：音声（10 ms 未満の遅延およびジッタ）
- 7：ネットワーク コントロール
- all：すべての優先度を一度に設定します。

（注） クライアントが使用する集約方法に合わせて優先度を設定します。

次に、2.4 GHz 帯域で 802.11n サポートを有効にする例を示します。

```
Device(config)# ap dot11 24ghz dot11n
```

次に、優先度レベルに関連付けられたトラフィックがA-MSDU伝送を使用するようにすべての優先度レベルを設定する例を示します。

```
Device(config)# ap dot11 24ghz dot11n a-msdu tx priority all
```

次に、長期ガード間隔だけを有効にする例を示します。

```
Device(config)# ap dot11 24ghz dot11n guard-interval long
```

次に、MCS レートを指定する例を示します。

```
Device(config)# ap dot11 24ghz dot11n mcs tx 5
```

次に、RIFS を有効にする例を示します。

```
Device(config)# ap dot11 24ghz dot11n rifs rx
```

ap dot11 dtpc

Dynamic Transmit Power Control（DTPC）設定、Cisco Client eXtension（CCX）バージョン 5 Expedited Bandwidth Request 機能、および 802.11 ネットワークのフラグメンテーションしきい値を指定するには、**apdot11dtpc** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} {**dtpc**| **exp-bwreq**| **fragmentation** *threshold*}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
dtpc	Dynamic Transport Power Control（DTPC）設定を指定します。 （注） このオプションは、デフォルトで有効です。
exp-bwreq	Cisco Client eXtension（CCX）バージョン 5 Expedited Bandwidth Request 機能を指定します。 （注） Expedited Bandwidth Request 機能はデフォルトでは無効になっています。
fragmentation*threshold*	フラグメンテーションしきい値を指定します。 （注） このオプションは、**apdot11** {**24ghz**	**5ghz**} **shutdown** コマンドを使用してネットワークが無効になっている場合にだけ使用できます。
threshold	しきい値。指定できる範囲は256～2346バイトです（両端の値を含む）。

コマンド デフォルト

なしーバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

CCX バージョン 5 Expedited Bandwidth Request 機能が有効になっている場合、デバイスは、この機能に関して、参加しているすべてのアクセス ポイントを設定します。

次に、5 GHz 帯域の DTPC を有効にする例を示します。

```
Device(config)# ap dot11 5ghz dtpc
```

次に、CCX Expedited Bandwidth 設定をイネーブルにする例を示します。

```
Device(config)# ap dot11 5ghz exp-bwrep
```

次に、5 GHz 帯域のフラグメンテーションしきい値を 1500 バイトのしきい値数で設定する例を示します。

```
Device(config)# ap dot11 5ghz fragmentation 1500
```

ap dot11 edca-parameters

2.4 GHz 帯域または 5 GHz 帯域で特定の Enhanced Distributed Channel Access（EDCA）プロファイルを有効にするには、**apdot11edca-parameters** コマンドを使用します。2.4 GHz 帯域または 5 GHz 帯域で EDCA プロファイルを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**} **edca-parameters** {**custom-voice**| **optimized-video-voice**| **optimized-voice**| **svp-voice**| **wmm-default**}

no ap dot11 {**24ghz**| **5ghz**} **edca-parameters** {**custom-voice**| **optimized-video-voice**| **optimized-voice**| **svp-voice**| **wmm-default**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
edca-parameters	802.11 ネットワークで特定の Enhanced Distributed Channel Access（EDCA）プロファイルを指定します。
custom-voice	カスタム音声 EDCA パラメータを有効にします。

optimized-video-voice	EDCA 音声/ビデオ最適化パラメータを有効にします。ネットワーク上で音声サービスとビデオサービスを両方とも展開する場合に、このオプションを選択します。
optimized-voice	EDCA 音声最適化パラメータを有効にします。ネットワーク上で SpectraLink 以外の音声サービスを展開する場合に、このオプションを選択します。
svp-voice	SpectraLink 音声優先パラメータを有効にします。コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。
wmm-default	Wi-Fi Multimedia（WMM）デフォルト パラメータを有効にします。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。

コマンド デフォルト

wmm-default

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
10.3	Cisco 5700 シリーズ WLC で **custom-voice** キーワードが削除されました。

次に、SpectraLink 音声優先パラメータを有効にする例を示します。

```
Device(config)# ap dot11 24ghz edca-parameters svp-voice
```

ap dot11 rrm group-mode

802.11 の自動 RF グループ選択モードをオンに設定するには、**apdot11rrmgroup-mode** コマンドを使用します。802.11 の自動 RF グループ選択モードをオフに設定するには、このコマンドの **no** 形式を使用します。

ap dot11 {**5ghz**| **24ghz**} **rrm group-mode** {**auto**| **leader**| **off**| **restart**}

no ap dot11 {**5ghz**| **24ghz**} **rrm group-mode**

構文の説明

5ghz	2.4 GHz 帯域を指定します。
24ghz	5 GHz 帯域を指定します。
auto	802.11 RF グループ選択を自動更新モードに設定します。
leader	802.11 RF グループ選択をスタティック モードに設定し、グループ リーダーとしてこのデバイスを設定します。
off	802.11 RF グループ選択をオフに設定します。
restart	802.11 RF グループ選択を再起動します。

コマンド デフォルト

auto

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、5 GHz 帯域の自動 RF グループ選択モードをオンにする例を示します。

```
Device(config)# ap dot11 5ghz rrm group-mode auto
```

ap dot11 rrm channel cleanair-event

すべての 802.11 Cisco Lightweight アクセス ポイントの CleanAir イベント駆動型無線リソース管理（RRM）パラメータを設定するには、**apdot11rrmchannelcleanair-event** コマンドを使用します。このパラメータが設定されている場合、CleanAir アクセス ポイントは、RRM 間隔が期限切れになっていなくても、干渉源によって動作が低下するとチャネルを変更できます。

構文の説明

24ghz	2.4 GHz 帯域を指定します。

ap dot11 {**24ghz**| **5ghz**} **rrm channel** {**cleanair-event sensitivity** *value*}

5ghz	5 GHz 帯域を指定します。
sensitivity	CleanAir イベント駆動型 RRM の感度を設定します。
value	感度の値。次の 3 つの感度値オプションのいずれかを選択できます。 • **low**：低感度を指定します。 • **medium**：中間の感度を指定します。 • **high**：高感度を指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、CleanAir イベント駆動型 RRM に高感度を設定する例を示します。

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

ap dot11 l2roam rf-params

2.4 GHz または 5 GHz のレイヤ 2 クライアント ローミング パラメータを設定するには、**apdot11l2roamrf-params** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **l2roam rf-params custom** *min-rssi roam-hyst scan-thresh trans-time*

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
custom	レイヤ 2 クライアントのカスタム ローミング RF パラメータを指定します。

min-rssi	クライアントをアクセス ポイントに関連付けるために必要な最小の受信信号強度インジケータ（RSSI）。クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。有効な範囲は -80 ～ -90 dBm で、デフォルト値は -85 dBm です。
roam-hyst	クライアントがローミングするために、周辺のアクセス ポイントの信号に必要な強度。このパラメータは、クライアントが 2 つのアクセス ポイント間のボーダー近くに物理的に存在している場合に、アクセス ポイント間のローミングの量を減らすことを意図しています。有効な範囲は 2 ～ 4 dB で、デフォルト値は 2 dB です。
scan-thresh	許容可能な最小 RSSI。この値を下回ると、クライアントはより適切なアクセス ポイントをローミングする必要があります。RSSI が指定された値より低い場合、クライアントは指定遷移時間内により強い信号のあるアクセス ポイントへローミングできる必要があります。このパラメータはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。有効な範囲は -70 ～ -77 dBm で、デフォルト値は -72 dBm です。
trans-time	クライアントのアソシエートされたアクセス ポイントからの RSSI がスキャンのしきい値を下回った場合に、クライアントがローミングに適したネイバー アクセス ポイントの検出と、ローミングの完了にかけられる最大許容時間。有効な範囲は 1 ～ 10 秒で、デフォルト値は 5 秒です。

コマンド デフォルト

min-rssi	-85
roam-hyst	2
scan-thresh	-72
trans-time	5

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、802.11a ネットワークにカスタム レイヤ 2 クライアント ローミング パラメータを設定する例を示します。

```
Device(config)# ap dot11 5ghz l2roam rf-params custom -80 2 -70 7
```

ap dot11 media-stream

802.11 ネットワークのメディア ストリームのマルチキャスト ダイレクト設定とビデオ ダイレクト設定を指定するには、**apdot11media-stream** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **media-stream** {**multicast-direct** {**admission-besteffort**| **client-maximum** *value*| **radio-maximum** *value*}| **video-redirect**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
multicast-direct	2.4 GHz 帯域または 5 GHz 帯域のマルチキャスト ダイレクトを指定します。
admission-besteffort	ベスト エフォート キューにメディア ストリームを許可します。
client-maximum*value*	クライアントで許可されるストリームの最大数を指定します。
radio-maximum*value*	2.4 GHz 帯域または 5 GHz 帯域で許可されるストリームの最大数を指定します。
video-redirect	2.4 GHz 帯域または 5 GHz 帯域のメディア ストリームのビデオ ダイレクトを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

802.11 ネットワークのメディア ストリームのマルチキャスト ダイレクトまたはビデオ ダイレクトを設定する前に、ネットワークが非動作であることを確認します。

次に、5 GHz 帯域でメディア ストリームのマルチキャスト ダイレクト設定を有効にする例を示します。

```
Device(config)# ap dot11 5ghz media-stream multicast-direct
```

次に、フローに順位付けするために十分な帯域幅がない場合に、ベストエフォート キューにメディア ストリームを許可さする例を示します。

```
Device(config)# ap dot11 5ghz media-stream multicast-direct admission-besteffort
```

次に、クライアントで許可される最大ストリーム数を設定する例を示します。

```
Device(config)# ap dot11 5ghz media-stream multicast-direct client-maximum 10
```

次に、5 GHz 帯域でメディア ストリーム トラフィック リダイレクションを有効にする例を示します。

```
Device(config)# ap dot11 5ghz media-stream video-redirect
```

ap dot11 rrm ccx location-measurement

2.4 GHz 帯域および 5 GHz 帯域の Cisco Client Extension（CCX）クライアント ロケーション測定を設定するには、**apdot11rrmccxlocation-measurement** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **rrm ccx location-measurement** {**disable**| *interval*}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
disable	CCX クライアント ロケーション測定のサポートを無効にします。

interval	間隔（10 ～ 32400）。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz の CCXクライアント ロケーション測定のサポートを無効にする例を示します。

```
Device(config)# no ap dot11 24ghz rrm ccx location-measurement
```

ap dot11 rrm channel dca

802.11 ネットワークの動的チャネル割り当て（DCA）アルゴリズム パラメータを設定するには、**apdot11rrmchanneldca** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **rrm channel dca**{*channel_number*| **anchor-time** *value*| **global**{**auto**| **once**}| **interval** *value*| **min-metric** *value*| **sensitivity**{**high**| **low**| **medium**}}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
channel_number	DCA リストに追加するチャネル番号。 （注） 範囲は 1 ～ 14 です。
anchor-time	DCA アンカー時間を指定します。
value	時間（0 ～ 23）。この値は、午前 12 時から午後 11 時までの時間を表します。

global	802.11 ネットワークのアクセス ポイントに対してグローバルな DCA モードを指定します。
auto	自動 RF を有効にします。
once	ワンタイム自動 RF を有効にします。
interval	DCA の実行が許可される頻度を指定します。
value	DCA が実行できる時間の間隔。有効な値は 0、1、2、3、4、6、8、12、または 24 時間です。0 の場合は 10 分になります（600 秒）。デフォルト値は 0（10 分）です。
min-metric	DCA の最小 RSSI エネルギー メトリックを指定します。
value	最小 RSSI エネルギー メトリック値（-100 ～ -60）。
sensitivity	DCA アルゴリズムでチャネルを変更するかどうかを判断する際の、環境の変化（信号、負荷、ノイズ、干渉など）に対する感度を指定します。
high	環境の変化に対する DCA アルゴリズムの感度は特に高くないことを指定します。詳細については、「使用上のガイドライン」を参照してください。
low	環境の変化に対する DCA アルゴリズムの感度は中程度であることを指定します。詳細については、「使用上のガイドライン」を参照してください。
medium	環境の変化に対する DCA アルゴリズムの感度が高いことを指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンド 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

トラブルシューティングに役立つように、このコマンドの出力には失敗したコールすべてのエラーコードが示されます。次の表では、失敗したコールの考えられるエラー コードについて説明します。

表 *27*：*DCA* 感度しきい値

感度	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

次に、2.4 GHz 帯域で午後 5 時に DCA の実行を開始するようにデバイスを設定する例を示します。

```
Device(config)# ap dot11 24ghz rrm channel dca anchor-time 17
```

次に、2.4 GHz 帯域で 10 分ごとに実行するように DCA アルゴリズムを設定する例を示します。

```
Device(config)# ap dot11 24ghz rrm channel dca interval 0
```

次に、2.4 GHz 帯域で DCA アルゴリズムの感度の値を low に設定する例を示します。

```
Device(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

ap dot11 rrm group-member

802.11 静的 RF グループのメンバを設定するには、**apdot11rrmgroup-member** コマンドを使用します。802.11 RF グループからメンバを削除するには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

no ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
controller-name	追加するデバイスの名前。
controller-ip	追加するデバイスの IP アドレス。

コマンド デフォルト

なしグローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、5 GHz 帯域 RF グループにデバイスを追加する例を示します。

```
Device(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

ap dot11 rrm logging

サポートされている 802.11 ネットワークのレポート ログを設定するには、**apdot11rrmlogging** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **rrm logging** {**channel**| **coverage**| **foreign**| **load**| **noise**| **performance**| **txpower**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
channel	チャネル変更ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
coverage	カバレッジ プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
foreign	外部干渉プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
load	負荷プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
noise	ノイズ プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
performance	パフォーマンス プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
txpower	中継電力変更ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、5 GHz ロギング チャネル選択モードをオンにする例を示します。

```
Device(config)# ap dot11 5ghz rrm logging channel
```

次に、5 GHz カバレッジ プロファイル違反ロギング選択モードをオンにする例を示します。

```
Device(config)# ap dot11 5ghz rrm logging coverage
```

次に、5 GHz 外部干渉プロファイル違反ロギング選択モードをオンにする例を示します。

```
Device(config)# ap dot11 5ghz rrm logging foreign
```

次に、5 GHz 負荷プロファイル ロギング モードをオンにする例を示します。

```
Device(config)# ap dot11 5ghz rrm logging load
```

次に、5 GHz ノイズ プロファイル ロギング モードをオンにする例を示します。

```
Device(config)# ap dot11 5ghz rrm logging noise
```

次に、5 GHz パフォーマンス プロファイル ロギング モードをオンにする例を示します。

```
Device(config)# ap dot11 5ghz rrm logging performance
```

次に、5 GHz 伝送パワー変更モードをオンにする例を示します。

```
Device(config)# ap dot11 5ghz rrm logging txpower
```

ap dot11 rrm monitor

802.11 ネットワークのモニタを設定するには、**apdot11rrmmonitor** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **rrm monitor**{**channel-list**| {**all**| **country**| **dca**}| **coverage**| **load**| **noise**| **signal**} *seconds*

構文の説明

24ghz	802.11b パラメータを指定します。
5ghz	802.11a パラメータを指定します。
channel-listall	すべてのチャネルのノイズ、干渉、不正モニタリング チャネル リストをモニタします。
channel-listcountry	設定されている国で使用するチャネルのノイズ、干渉、不正モニタリング チャネル リストをモニタします。

channel-listdca	自動チャネル割り当てによって使用されるチャネルのノイズ、干渉、不正モニタリング チャネル リストをモニタします。
coverage	カバレッジ測定間隔を指定します。
load	負荷測定間隔を指定します。
noise	ノイズ測定間隔を指定します。
signal	信号測定間隔を指定します。
rssi-normalization	RRM ネイバー探索 RSSI 正規化を設定します。
seconds	測定間隔は 60 ～ 3600 秒です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、設定されている国で使用するチャネルを監視する例を示します。

```
Device(config)# ap dot11 24ghz rrm monitor channel-list country
```

次に、カバレッジ測定間隔を 60 秒に設定する例を示します。

```
Device(config)# ap dot11 24ghz rrm monitor coverage 60
```

ap dot11 rrm ndp-type

802.11 アクセスポイント無線リソース管理ネイバー ディスカバリ プロトコル タイプを設定するには、**apdot11rrmndp-type** コマンドを使用します。

構文の説明

ap dot11 {**24ghz**| **5ghz**} **rrm ndp-type** {**protected**| **transparent**}

24ghz	2.4 GHz 帯域を指定します。

5ghz	5 GHz 帯域を指定します。
protected	Tx RRM で保護された（暗号化された）ネイバー ディスカバリ プロトコルを指定します。
transparent	Tx RRM の透過的な（暗号化されていない）ネイバー ディスカバリ プロトコルを指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

802.11 アクセス ポイント RRM のネイバー ディスカバリ プロトコル タイプを設定する前に、**apdot11 {24ghz | 5ghz} shutdown** コマンドを入力してネットワークを無効にしていることを確認してください。

次に、802.11a アクセス ポイント RRM ネイバー ディスカバリ プロトコル タイプを protected として有効にする例を示します。

```
Device(config)# ap dot11 5ghz rrm ndp-type protected
```

ap dot11 5ghz dot11ac frame-burst

802.11ac フレームバーストを設定するには、**apdot115ghzdot11acframe-burst** コマンドを使用します。802.11ac A-MPDU のバースティングを無効にするには、このコマンドの **no** 形式を使用します。

ap dot115ghzdot11acframe-burst

noap dot115ghzdot11acframe-burst

ap dot115ghzdot11acframe-burstautomatic

noap dot115ghzdot11acframe-burstautomatic

構文の説明

5ghz	802.11a パラメータを設定します。
frame-burst	802.11ac A-MPDU のバースティングを設定します。

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
Cisco IOS XE 3.6E	このコマンドが導入されました。

例

次に、802.11ac A-MPDU のバースティングを設定する例を示します。

```
Deviceap dot11 5ghz
  dot11ac frame-burst
```

ap dot1x max-sessions

各アクセス ポイントに許可されている同時 802.1X セッションの最大数を設定するには、**apdot1xmax-sessions** コマンドを使用します。

ap dot1x max-sessions *num-of-sessions*

構文の説明

num-of-sessions	一度の AP あたりの 802.1X セッション開始の最大数。範囲は 0～255 で、0 は無制限を示します。

コマンド デフォルト

なし グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

802.1Xメッセージを使用によって発生するフラッディング攻撃から保護するために、アクセスポイントごとに開始される同時 802.1X セッションの数を制限する必要があります。

次に、同時 802.1X セッションの最大数を設定する例を示します。

```
Device(config)# ap dot1x max-sessions 100
```

ap dot1x username

現在デバイスに参加しているすべてのアクセスポイントと今後デバイスに参加するアクセスポイントの 802.1X ユーザ名およびパスワードを設定するには、**apdot1xusername** コマンドを使用します。現在デバイスに参加しているすべてのアクセスポイントの802.1Xユーザ名およびパスワードを無効にするには、このコマンドの **no** 形式を使用します。

ap dot1x username *user-id* **password**{**0**| **8**} *password-string*

no ap dot1x username *user-id***password**{**0**| **8**} *password-string*

構文の説明

user-id	ユーザ名。
password	すべてのアクセス ポイントの 802.1X パスワードを指定します。
0	暗号化されていないパスワードを指定します。
8	AES 暗号化パスワードを指定します。
password_string	パスワード。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

強度が高いパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

特定のアクセス ポイントの値を設定できます。

次に、すべてのアクセス ポイントにグローバル認証ユーザ名およびパスワードを設定する例を示します。

```
Device(config)# ap dot1x username cisco123 password 0 cisco2020
```

ap ethernet duplex

Lightweightアクセス ポイントのイーサネット ポート デュプレックスおよび速度を設定するには、**apethernetduplex** コマンドを使用します。Lightweight アクセス ポイントのイーサネット ポート デュプレックスおよび速度を無効にするには、このコマンドの **no** 形式を使用します。

ap ethernet duplex *duplex* **speed** *speed*

no ap ethernet

構文の説明

duplex	イーサネット ポートのデュプレックス設定。次のオプションを指定してデュプレックスを設定できます。 • **auto**：イーサネット ポートの自動二重設定を指定します。 • **half**：イーサネット ポートの半二重設定を指定します。 • **full**：イーサネット ポートの全二重設定を指定します。

speed	イーサネット ポート速度の設定を指定します。
speed	イーサネット ポートの速度設定。次のオプションを指定して速度を設定できます。 • **auto**：イーサネット ポート速度を自動に指定します。 • **10**：イーサネット ポート速度を 10 Mbps に指定します。 • **100**：イーサネット ポート速度を 100 Mbps に指定します。 • **1000**：イーサネット ポート速度を 1000 Mbps に指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントで 1000 Mbps としてイーサネット ポートの全二重を設定する例を示します。

```
Device(config)# ap ethernet duplex full speed 1000
```

ap group

新しいアクセス ポイント グループを作成するには、**apgroup** コマンドを使用します。アクセス ポイント 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。

ap group *group-name*

構文の説明

no ap group *group-name* *group-name*	アクセス ポイント グループ名。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

1 つ以上のアクセス ポイントで使用しているアクセス ポイント グループを削除しようとすると、エラー メッセージが表示されます。AP グループを削除するには、まず、このグループのすべての AP を別のグループに移動します。アクセス ポイントが default-group アクセス ポイント グループに自動的に移動されることはありません。AP を表示するには、**showapsummary** コマンドを入力します。アクセス ポイントを移動するには、**apname***Cisco-AP***ap-groupname***Group-Name* コマンドを入力します。

次に、新しいアクセス ポイント グループを作成する例を示します。

```
Device(config)# ap group sampleapgroup
```

ap image

デバイスに関連付けられているすべてのアクセス ポイントでイメージを設定するには、**apimage** コマンドを使用します。

ap image {**predownload| reset| swap**}

構文の説明

predownload	すべてのアクセスポイントにイメージのプレダウンロードを開始するように指示します。
reset	すべてのアクセス ポイントに再起動するように指示します。
swap	すべてのアクセス ポイントにイメージを切り替えるように指示します。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントにイメージをプレダウンロードする例を示します。

```
Device# ap image predownload
```

次に、すべてのアクセス ポイントを再起動する例を示します。

```
Device# ap image reset
```

次に、アクセス ポイントのプライマリ イメージとセカンダリ イメージを切り替える例を示します。

```
Device# ap image swap
```

ap ipv6 tcp adjust-mss

すべてのシスコ AP の IPv6 TCP 最大セグメント サイズ（MSS）値を設定するには、**ap ipv6 tcp adjust-mss** コマンドを使用します。

ap ipv6 tcp adjust-mss *size*

no ap ipv6 tcp adjust-mss *size*

構文の説明

adjust-mss	すべてのシスコ AP の IPv6 TCP MSS を設定します。
size	MSS 値（500 ～ 1440）。

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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

MSS 値は 500 ～ 1440 の範囲でなければなりません。

次に、すべてのシスコ アクセス ポイントの IPv6 TCP MSS 値を 600 に設定する例を示します。

```
Device(config)# ap ipv6 tcp adjust-mss 600
```

ap led

アクセス ポイントの LED ステートを有効にするには、**apled** コマンドを使用します。アクセス ポイントの LED ステートを無効にするには、このコマンドの **no** 形式を使用します。

ap led

no ap led

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの LED ステートを有効にする例を示します。

```
Device(config)# ap led
```

ap link-encryption

アクセス ポイントの Datagram Transport Layer Security（DTLS）データ暗号化を有効にするには、**aplink-encryption** コマンドを使用します。アクセス ポイントの DTLS データ暗号化を無効にするには、このコマンドの **no** 形式を使用します。

ap link-encryption

no ap link-encryption

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、コントローラに参加しているすべてのアクセス ポイントのデータ暗号化を有効にする例を示します。

```
Device(config)# ap link-encryption
```

ap link-latency

デバイスに現在関連付けられているすべてのアクセスポイントのリンク遅延を有効にするには、**aplink-latency** コマンドを使用します。デバイス に現在関連付けられているすべてのアクセス ポイントのリンク遅延を無効にするには、このコマンドの **no** 形式を使用します。

ap link-latency [**reset**]

no ap link-latency

構文の説明

reset	（任意）すべてのアクセス ポイントのリンク遅延をリセットします。

コマンド デフォルト

リンク遅延は、デフォルトでは無効になります。

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
Cisco IOS XE 3.2SE	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、現在デバイスに参加しているアクセス ポイントだけに対してリンク遅延を有効または無効にします。将来参加するアクセス ポイントには適用されません。

次に、すべてのアクセス ポイントのリンク遅延を有効にする例を示します。

```
Device(config)# ap link-latency
```

ap mgmtuser username

アクセス ポイント管理用のユーザ名、パスワード、シークレット パスワードを設定するには、**apmgmtuserusername** コマンドを使用します。

ap mgmtuser username *username* **password** *password_type password* **secret** *secret_type secret*

構文の説明

username	アクセス ポイント管理用のユーザ名を指定します。
password	アクセス ポイント管理用のパスワードを指定します。

password_type	パスワードタイプ。次の2つのパスワードタイプのいずれかを指定できます。 • **0**：暗号化されていないパスワードが後に続くことを示します。 • **8**：AES 暗号化パスワードが続くことを指定します。
password	アクセス ポイント管理パスワード。 （注） パスワードは、サービス パスワード暗号化によって暗号化されません。
secret	特権アクセス ポイント管理用のシークレット パスワードを指定します。
secret_type	シークレットタイプ。次の2つのシークレットタイプのいずれかを指定できます。 • **0**：暗号化されていないシークレット パスワードが後に続くことを示します。 • **8**：AES 暗号化シークレット パスワードが続くことを指定します。
secret	アクセス ポイント管理シークレット パスワード。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

強力なパスワードを指定するには、次のパスワード要件を満たす必要があります。

- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。
- パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
- パスワードに管理ユーザ名や逆にしたユーザ名を含めることはできません。
- パスワードに使用しないほうがよい文字には、Cisco、oscic、admin、nimda などの語のほか、大文字の代わりに 1 や|、！を、o の代わりに 0 を、s の代わりに $ を使用して置き換えた文字などがあります。

強力なシークレット パスワードを指定するには、次の要件を満たす必要があります。

- シークレット パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。

次に、アクセスポイント管理用のユーザ名、パスワード、シークレットパスワードを追加する例を示します。

```
Device(config)# ap mgmtuser username glbusr password 0 Arc_1234 secret 0 Mid_1234
```

ap name ap-groupname

特定のアクセス ポイント グループに Cisco Lightweight アクセス ポイントを追加するには、**apnameap-groupname** コマンドを使用します。

ap name *ap-name* **ap-groupname** *group-name*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
group-name	アクセス ポイント グループの内容がわかる名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

Cisco Lightweight アクセス ポイントを無効にしてから、このパラメータを変更する必要があります。

次に、アクセス ポイント AP01 をアクセス ポイント グループ スーパーユーザに追加する例を示します。

```
Device# ap name AP01 ap-groupname superusers
```

ap name antenna band mode

アンテナ モードを設定するには、**ap name<AP name> antenna-band-mode{ single | dual }** コマンドを使用します。

ap name*ap-name***antenna-band-mode**{**single**| **dual**}

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
antenna-band-mode	アクセスポイントにアンテナのバンドモードを有効にするように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、アクセス ポイントのアンテナ バンド モードを設定する例を示します。

```
Deviceap name <ap-name> antenna-band-mode single
```

ap name bhrate

Cisco Bridge Backhaul Tx Rate を設定するには、**apnamebhrate** コマンドを使用します。

ap name *ap-name* **bhrate** *kbps*

構文の説明

ap-name	Cisco アクセス ポイントの名前。
kbps	Cisco Bridge Backhaul Tx Rate（Kbps）。有効な値は、6000、12000、18000、24000、36000、48000、および 54000 です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、Cisco Bridge Backhaul Tx Rate を 54000 kbps に設定する例を示します。

```
Device# ap name AP02 bhrate 54000
```

ap name bridgegroupname

Cisco Lightweight アクセス ポイントでブリッジ グループ名を設定するには、**apnamebridgegroupname** コマンドを使用します。Cisco Lightweight アクセス ポイントでブリッジ グループ名を削除するには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **bridgegroupname** *bridge_group_name*

ap name *ap-name* **no bridgegroupname**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

同じブリッジ グループ名を持つアクセス ポイントだけが相互に接続できます。アクセス ポイントのブリッジ グループ名を変更すると、ブリッジ アクセス ポイントが機能しなくなる場合があります。

次に、Cisco アクセス ポイントのブリッジ グループ名 AP02 でブリッジ グループ名を設定する例を示します。

```
Device# ap name AP02 bridgegroupname West
```

次に、Cisco アクセス ポイントのブリッジ グループ名 AP02 でブリッジ グループ名を削除する例を示します。

```
Device# ap name AP02 no bridgegroupname
```

ap name bridging

Cisco Lightweight アクセス ポイントでイーサネット間ブリッジングを有効にするには、**apnamebridging** コマンドを使用します。Cisco Lightweight アクセス ポイントでイーサネット間ブリッジングを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **bridging**

ap name *ap-name* **no bridging**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントでイーサネット間ブリッジングを有効にする例を示します。

```
Device# ap name TSIM_AP2 bridging
```

ap name cdp interface

Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を有効にするには、**apname** コマンドを使用します。Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **cdp interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}

ap name *ap-name* [**no**] **cdp interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
ethernet	イーサネット インターフェイス上で CDP を有効にします。
ethernet-id	イーサネット インターフェイス番号（0 ～ 3）。
radio	無線インターフェイスの CDP を有効にします。
radio-id	無線 ID スロット番号（0 ～ 3）。

コマンド デフォルト

すべてのアクセス ポイントで無効になっています。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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/無線インターフェイス上の CDP は、CDP が有効になっている場合にだけ使用できます。デバイスに参加しているすべてのアクセス ポイントで CDP を有効にした後は、**apname***ap-name***cdpinterfaceethernet***ethernet-id* cisco_ap コマンドを使用して、個々のアクセス ポイントで CDP を無効にし、再度有効にすることができます。デバイスに参加しているすべてのアクセス ポイントで CDP を無効にした後は、個々のアクセス ポイントで CDP を有効にし、無効にすることはできません。

次に、アクセス ポイントでイーサネット インターフェイス番号 0 の CDP を有効にする例を示します。

```
Device# ap name TSIM_AP2 cdp interface ethernet 0
```

ap name console-redirect

Cisco Lightweight アクセス ポイントのリモート デバッグ出力をコンソールにリダイレクトするには、**apnameconsole-redirect** コマンドを使用します。Cisco Lightweight アクセス ポイントのリモート デバッグ出力のコンソールへのリダイレクトを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **console-redirect**

ap name *ap-name* [**no**] **console-redirect**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、AP02 というシスコのアクセス ポイントのリモート デバッグ出力のコンソールへのリダイレクトを有効にする例を示します。

```
Device# ap name AP02 console-redirect
```

ap name capwap retransmit

アクセス ポイント制御パケットの再送信間隔と制御パケットの再送信回数を設定するには、**apnamecapwapretransmit** コマンドを使用します。

ap name *ap-name* **capwap retransmit** {**count** *count-value*| **interval** *interval-time*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
count	制御パケットが再送信される回数を設定します。
count-value	制御パケットが再送信される回数（3 ～ 8）。
interval	制御パケットの再送信タイムアウト間隔を設定します。
interval-time	制御パケットの再送信タイムアウト（2 ～ 5 秒）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの再送信間隔を設定する例を示します。

```
Device# ap name AP01 capwap retransmit interval 5
```

次に、特定のアクセス ポイントに対する再送信の再試行回数を設定する例を示します。

```
Device# ap name AP01 capwap retransmit count 5
```

ap name command

特定のシスコのアクセス ポイントでコマンドをリモート実行するには、**apnamecommand** コマンドを使用します。

ap name *ap-name* **command**"*command* "

構文の説明

ap-name	Cisco アクセス ポイントの名前。
command	シスコのアクセス ポイントで実行するコマンド。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、TSIM_AP2 という シスコのアクセス ポイントに **show ip interface brief** コマンドをリモート入力する例を示します。

```
Device# ap name AP2 command "show ip interface brief"
```

ap name core-dump

Cisco Lightweight アクセス ポイントのメモリ コア ダンプを設定するには、**apnamecore-dump** コマンドを使用します。Cisco Lightweight アクセス ポイントのメモリ コア ダンプを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **core-dump** *tftp-ip-addr filename* {**compress**| **uncompress**}

ap name *ap-name* [**no**]**core-dump**

構文の説明

ap-name	アクセス ポイントの名前。
tftp-ip-addr	アクセス ポイントがコア ダンプ ファイルを送信する Trivial File Transfer Protocol（TFTP）サーバの IP アドレス。
filename	コア ファイルのラベルを付けるためにアクセス ポイントが使用する名前。
compress	コア ダンプ ファイルを圧縮します。
uncompress	コア ダンプ ファイルを圧縮解除します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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には、アクセス ポイントが TFTP サーバに到達できる必要があります。

次に、コア ダンプ ファイルを設定して圧縮する例を示します。

```
Device# ap name AP2 core-dump 192.1.1.1 log compress
```

ap name country

Cisco Lightweight アクセス ポイントを使用する国を設定するには、**apnamecountry** コマンドを使用します。

ap name *ap-name* **country** *country-code*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
country-code	2 文字または 3 文字の国コード。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

Cisco デバイス は、ネットワーク管理者または資格のある IP プロフェッショナルがインストールしてください。その際、正しい国コードを選択する必要があります。インストール後は、法的な規制基準を遵守するためおよび、適切なユニット機能を保証するために、ユニットへのアクセスはパスワードで保護する必要があります。最新の国コードおよび規制区域については、関連する製品マニュアルを参照してください。また、アクセスポイントの規制区域は、アクセスポイントの製造プロセス中に定義されます。アクセスポイントの国コードは、アクセスポイントの規制区域内で有効な国と一致する国コードに変更できます。アクセス ポイントの規制区域に対して有効でない国を入力しようとすると、コマンドは失敗します。

次に、Cisco Lightweight アクセス ポイントの国コードを DE に設定する例を示します。

```
Device# ap name AP2 country JP
```

ap name crash-file

シスコのアクセス ポイントのクラッシュ データおよび無線コア ファイルを管理するには、**apnamecrash-file** コマンドを使用します。

ap name *ap-name* **crash-file** {**get-crash-data**| **get-radio-core-dump** {**slot 0**| **slot 1**}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
get-crash-data	Cisco Lightweight アクセス ポイントの最新のクラッシュ データを収集します。
get-radio-core-dump	Cisco Lightweight アクセス ポイントの無線コア ダンプを取得します。
slot	シスコのアクセス ポイントのスロット ID。
0	スロット 0 を指定します。
1	スロット 1 を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント A3 の最新のクラッシュ データを収集する例を示します。

```
Device# ap name AP3 crash-file get-crash-data
```

次に、アクセス ポイント AP02 とスロット 0 の無線コア ダンプを収集する例を示します。

```
Device# ap name AP02 crash-file get-radio-core-dump slot 0
```

ap name dot11 24ghz rrm coverage

2.4 GHz 帯域でカバレッジ ホール検出を設定するには、**apnamedot1124ghzrrmcoverage** コマンドを使用します。

ap name *ap-name* **dot11 24ghz rrm coverage** {**exception** *value*| **level** *value*}

構文の説明

ap-name	Cisco アクセス ポイントの名前。
exception	アクセス ポイント上で、信号レベルが低くなっているにもかかわらず、別のアクセス ポイントにローミングできないクライアントの割合を指定します。
value	クライアントの割合。有効な値は 0 ～ 100 % です。 （注） デフォルトは 25% です。
level	アクセス ポイント上でデータまたは音声 RSSI しきい値以下の受信信号強度表示（RSSI）値を持つクライアントの最小数を指定します。
value	クライアントの最小数。有効な値は 1 ～ 75 です。 （注） デフォルトは 3 です。

コマンド デフォルト

exception パラメータのデフォルトは 25%、*level* パラメータのデフォルトは 3 です。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

カバレッジ ホール検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセスポイントがあるかどうかを、アクセスポイントから受信したデータに基づいてデバイスが自動的に判断します。

失敗したパケットの数と数の両方が、**apdot1124ghzrrmcoveragedatapacket-count***count* コマンドと **apdot1124ghzrrmcoveragedatafail-percentage***percentage* コマンドで入力した値を 5 秒間超えると、クライアントは事前アラーム状態と見なされます。デバイスは、この情報を使用してカバレッジ ホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。失敗したクライアントの数と割合の両方が、90 秒以上にわたって、**apdot1124ghzrrmcoverageexception** コマンドと **apdot1124ghzrrmcoveragelevel** コマンドで入力した値以上になると、カバレッジ ホールが検出されます。デバイスは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、信号レベルが低くなっている 2.4 GHz 無線アクセス ポイントにクライアントの割合を指定する例を示します。

```
Device# ap name AP2 dot11 24ghz rrm coverage exception 25%
```

次に、RSSI しきい値以下の RSSI 値を持つ 802.11b アクセス ポイントでクライアントの最小数を指定する例を示します。

```
Device# ap name AP2 dot11 24ghz rrm coverage level 60
```

ap name dot11 49ghz rrm profile

4.9G Hz パブリック セーフティ チャネル上の Cisco Lightweight アクセス ポイントの無線リソース管理（RRM）パフォーマンス プロファイルを設定するには、**apnamedot1149ghzrrmprofile** コマンドを使用します。

ap name *ap-name* **dot11 49ghz rrm profile** {**clients** *value*| **customize**| **exception** *value*| **foreign** *value*| **level** *value*| **noise** *value*| **throughput** *vaue*| **utilization** *value*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
clients	アクセス ポイント クライアントしきい値を設定します。
value	アクセス ポイント クライアントしきい値（1 ～ 75 クライアント）。 （注） デフォルトのクライアントしきい値は 12 です。

customize	アクセス ポイントのパフォーマンス プロファイルのカスタマイズをオンにします。 （注） デフォルトでは、パフォーマンス プロファイルのカスタマイズはオフになっています。
exception*value*	シスコの 802.11a 対応アクセス ポイントのカバレッジ例外レベルを設定します（0 ー 100 □）。
foreign	外部 802.11 トランスミッタ干渉しきい値を設定します。
value	外部 802.11 トランスミッタ干渉しきい値（0 ～ 100 %）。 （注） デフォルトは 10 % です。
level*value*	シスコの 802.11a 対応アクセス ポイントのクライアント最小例外レベルを設定します（1 ー 75 クライアント）。
noise	802.11 外部ノイズしきい値を設定します。
value	802.11 外部ノイズしきい値（-127 ～ 0 dBm）。 （注） デフォルトは -70 dBm です。
throughput	データ レート スループットしきい値を設定します。
value	802.11 スループットしきい値（1000 ～ 10000000 バイト/秒） （注） デフォルトは、1,000,000 バイト/秒です。
utilization	RF 使用率しきい値を設定します。 （注） オペレーティング システムがこのしきい値を超えた場合にトラップを生成します。
value	802.11 RF使用率しきい値（0 ～ 100 %）。 （注） デフォルトは 80% です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、AP1 のクライアント数のしきい値を 75 個のクライアントに設定する例を示します。

```
Device# ap name AP1 dot11 49ghz rrm profile clients 75
```

次に、4.9 GHz チャネル上の Cisco Lightweight アクセス ポイント AP1 のパフォーマンス プロファイルのカスタマイズをオンにする例を示します。

```
Device# ap name AP1 dot11 49ghz rrm profile customize
```

次に、AP1 の外部トランスミッタ干渉しきい値を 0 パーセントに設定する例を示します。

```
Device# ap name AP1 dot11 49ghz rrm profile foreign 0
```

次に、AP1 の外部ノイズしきい値を 0 dBm に設定する例を示します。

```
Device# ap name AP1 dot11 49ghz rrm profile noise 0
```

次に、AP1 のデータ レートしきい値を 10,000,000 バイト/秒に設定する例を示します。

```
Device# ap name AP1 dot11 49ghz rrm profile throughput 10000000
```

次に、AP1 の RF 利用率のしきい値を 100 パーセントに設定する例を示します。

```
Device# ap name AP1 dot11 49ghz rrm profile utilization 100
```

ap name dot11 5ghz rrm channel

802.11h チャネル アナウンスを使用して新しいチャネルを設定するには、**apnamedot115ghzrrmchannel** コマンドを使用します。

ap name *ap-name* **dot11 5ghz rrm channel** *channel*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
channel	新しいチャネル。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、802.11h チャネルを使用して新しいチャネルを設定する例を示します。

```
Device# ap name AP01 dot11 5ghz rrm channel 140
```

ap name dot11 antenna

異なる 802.11 ネットワーク上の Cisco Lightweight アクセス ポイントの無線アンテナを設定するには、**apnamedot11antenna** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **antenna** {**ext-ant-gain** *gain*| **mode** {**omni**| **sectorA**| **sectorB**}| **selection** {**external**| **internal**}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
ext-ant-gain	802.11 ネットワークの外部アンテナ ゲインを指定します。 （注） このコマンドを入力する前に、**apdot11** {**24ghz**｜**5ghz**} **shutdown** コマンドを使用してシスコの無線を無効にしてください。このコマンドを入力した後に、**noapdot11** {**24ghz**｜**5ghz**} **shutdown** コマンドを使用してシスコの無線を再度有効にできます。
gain	0.5 dBm 単位でアンテナ ゲインを入力します（例：2.5 dBm = 5）。
mode	Cisco Lightweight アクセス ポイントが、802.11 の 180 度セクター化カバレッジ パターンに 1 つの内部アンテナを、または 802.11 の 360 度全方向性カバレッジ パターンに両方の内部アンテナを使用するように指定します。
omni	両方の内部アンテナを使用するように指定します。
sectorA	サイド A の内部アンテナだけを使用するように指定します。
sectorB	サイド B の内部アンテナだけを使用するように指定します。

selection	802.11 ネットワーク上の Cisco Lightweight アクセス ポイントの内部または外部アンテナ選択を指定します。
external	外部アンテナを指定します。
internal	内部アンテナを指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、5 GHz 外部アンテナ ゲインとして 0.5 dBm を AP1 に設定する例を示します。

```
Device# ap name AP1 dot11 5ghz antenna ext-ant-gain 0.5
```

次に、2.4 GHz 帯域上でアクセス ポイント AP01 のアンテナを 360 度全方向性パターンに設定する例を示します。

```
Device# ap name AP01 dot11 24ghz antenna mode omni
```

次に、2.4 GHz 帯域上のアクセス ポイント AP02 が内部アンテナを使用するように設定する例を示します。

```
Device# ap name AP02 dot11 24ghz antenna selection interval
```

ap name dot11 antenna extantgain

4.9G Hz および 5.8 GHz パブリック セーフティ チャネル上の Cisco Lightweight アクセス ポイントの無線アンテナを設定するには、**apnamedot11antennaextantgain** コマンドを使用します。

ap name *ap-name* **dot11** {**49ghz**| **58ghz**} {**antenna extantgain** *gain*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

49ghz	4.9 GHz パブリック セーフティ チャネル設定を指定します。
58ghz	5.8 GHz パブリック セーフティ チャネル設定を指定します。
gain	0.5 dBm 単位でアンテナ ゲインを入力します（例：2.5 dBm = 5）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、**apdot11** {**24ghz**|**5ghz**} **shutdown** コマンドを使用してシスコの無線を無効にしてください。このコマンドを入力した後に、**noapdot11** {**24ghz**|**5ghz**} **shutdown** コマンドを使用してシスコの無線を再度有効にできます。

次に、外部アンテナ ゲインとして 0.5 dBm を 4.9 GHz パブリック セーフティ チャネル上の AP1 に設定する例を示します。

```
Device# ap name AP1 dot11 49ghz antenna extantgain 0.5
```

ap name dot11 cleanair

802.11 ネットワーク上の特定の Cisco Lightweight アクセス ポイントの CleanAir を設定するには、**apnamedot11cleanair** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **cleanair**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。

5ghz	5 GHz 帯域を指定します。

コマンド デフォルト

ディセーブル

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz 帯域で CleanAir を有効にする例を示します。

```
Device# ap name AP01 dot11 24ghz cleanair
```

ap name dot11 dot11n antenna

特定のアンテナを使用するようにアクセス ポイントを設定するには、**apnamedot11dot11nantenna** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **dot11n antenna** {**A**| **B**| **C**| **D**}

構文の説明

ap-name	アクセス ポイント名。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
A	アンテナ ポート A を指定します。
B	アンテナ ポート B を指定します。
C	アンテナ ポート C を指定します。
D	アンテナ ポート D を指定します。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント AP02 でアンテナ B を有効にする例を示します。

```
Device# ap name AP02 dot11 5ghz dot11n antenna B
```

次に、アクセス ポイント AP02 でアンテナ C を無効にする例を示します。

```
Device# ap name AP02 no dot11 5ghz dot11n C
```

ap name dot11 dual-band cleanair

デュアルバンド無線の CleanAir を設定するには、**ap name dot11 dual-band cleanair** コマンドを使用します。

ap name *ap-name* **dot11 dual-band cleanair**

ap name *ap-name* **no dot11 dual-band cleanair**

構文の説明

ap-name	Cisco AP の名前。
cleanair	CleanAir 機能を指定します。

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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、アクセス ポイント AP01 のデュアルバンド無線の CleanAir を有効にする例を示します。

```
Device# ap name AP01 dot11 dual-band cleanair
```

ap name dot11 dual-band shutdown

シスコの AP でデュアルバンド無線を無効にするには、**ap name dot11 dual-band shutdown** コマンドを使用します。

ap name *ap-name* **dot11 dual-band shutdown**

ap name *ap-name* **no dot11 dual-band shutdown**

構文の説明

ap-name	Cisco AP の名前。
shutdown	シスコの AP でデュアルバンド無線を無効にします。

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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、シスコのアクセス ポイント AP01 でデュアルバンド無線を無効にする例を示します。

```
Device# ap name AP01 dot11 dual-band shutdown
```

ap name dot11 rrm ccx

802.11 ネットワークで特定の Cisco Lightweight アクセス ポイントの Cisco Client eXtension（CCX）無線リソース管理（RRM）を設定するには、**apnamedot11rrmccx** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **rrm ccx** {**customize**| **location-measurement** *interval*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
customize	802.11 CCX オプションを有効にします。
location-measurement	CCX クライアント ロケーション測定を設定します。
interval	間隔（10 ～ 32400）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz 帯域のアクセス ポイントの CCX クライアント ロケーション測定を設定する例を示します。

```
Device# ap name AP01 dot11 24ghz rrm ccx location-measurement 3200
```

ap name dot11 rrm profile

Cisco Lightweight アクセス ポイントの無線リソース管理（RRM）パフォーマンス プロファイルを設定するには、**apnamedot11rrmprofile** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **rrm profile** {**clients** *value*| **customize**| **foreign** *value*| **noise** *value*| **throughput** *value*| **utilization** *value*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。

5ghz	5 GHz 帯域を指定します。
clients	アクセス ポイント クライアントしきい値を設定します。
value	アクセス ポイント クライアントしきい値（1 ～ 75 クライアント）。 （注） デフォルトのクライアントしきい値は 12 です。
customize	アクセス ポイントのパフォーマンス プロファイルのカスタマイズをオンにします。 （注） デフォルトでは、パフォーマンス プロファイルのカスタマイズはオフになっています。
foreign	外部 802.11 トランスミッタ干渉しきい値を設定します。
value	外部 802.11 トランスミッタ干渉しきい値（0 ～ 100 %）。 （注） デフォルトは 10 % です。
noise	802.11 外部ノイズしきい値を設定します。
value	802.11 外部ノイズしきい値（-127 ～ 0 dBm）。 （注） デフォルトは -70 dBm です。
throughput	データ レート スループットしきい値を設定します。
value	802.11 スループットしきい値（1000 ～ 10000000 バイト/秒） （注） デフォルトは、1,000,000 バイト/秒です。
utilization	RF 使用率しきい値を設定します。 （注） オペレーティング システムがこのしきい値を超えた場合にトラップを生成します。
value	802.11 RF使用率しきい値（0 ～ 100 %）。 （注） デフォルトは 80% です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、AP1 のクライアント数のしきい値を 75 個のクライアントに設定する例を示します。

```
Device# ap name AP1 dot11 24ghz rrm profile clients 75
```

次に、802.11a 対応 Cisco Lightweight アクセス ポイント AP1 のパフォーマンス プロファイルのカスタマイズをオンにする例を示します。

```
Device# ap name AP1 dot11 5ghz rrm profile customize
```

次に、AP1 の外部 802.11a トランスミッタ干渉しきい値を 0 パーセントに設定する例を示します。

```
Device# ap name AP1 dot11 5ghz rrm profile foreign 0
```

次に、AP1 の 802.11a 外部ノイズしきい値を 0 dBm に設定する例を示します。

```
Device# ap name AP1 dot11 5ghz rrm profile noise 0
```

次に、AP1 のデータ レートしきい値を 10,000,000 バイト/秒に設定する例を示します。

```
Device# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

次に、AP1 の RF 利用率のしきい値を 100 パーセントに設定する例を示します。

```
Device# ap name AP1 dot11 5ghz rrm profile utilization 100
```

ap name dot11 txpower

802.11 ネットワーク内の単一のアクセス ポイントの送信電力レベルを設定するには、**apnamedot11txpower** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} {**shutdown**| **txpower** {**auto**| *power-level*}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
shutdown	802.11 ネットワークを無効にします。
auto	シスコの 802.11 対応無線の電力レベルが無線リソース管理（RRM）によって自動的に設定されるように指定します。

power-level	アクセス ポイントに手動で設定する送信電力レベルの数値。

コマンド デフォルト

コマンドのデフォルト（txpower auto）は RRM による自動設定用です。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント AP1 で 2.4 GHz 無線送信電力を自動的に設定する例を示します。

```
Device# ap name AP1 dot11 24ghz txpower auto
```

ap name dot1x-user

現在デバイスに参加しているアクセスポイントのグローバル認証ユーザ名およびパスワードを設定するには、**apnamedot1x-user** コマンドを使用します。特定のアクセス ポイントの 802.1X 認証を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **dot1x-user** {**global-override**| **username** *user-id* **password** *passwd*}

ap name *ap-name* [**no**] **dot1x-user**

構文の説明

ap-name	アクセス ポイントの名前。
global-override	アクセスポイントがデバイスのグローバル認証設定を使用するように強制します。
username	ユーザ名を追加することを指定します。
user-id	ユーザ名。
password	パスワードを追加することを指定します。
passwd	パスワード。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

強度が高いパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

  特定のアクセス ポイントの値を設定できます。

特定のアクセス ポイントの 802.1X 認証は、グローバル 802.1X 認証が有効でない場合にだけ無効にできます。グローバル 802.1X 認証が有効な場合は、すべてのアクセス ポイントに対してだけ 802.1X を無効にできます。

次に、dot1x 認証用に特定のユーザ名とパスワードを設定する例を示します。

```
Device# ap name AP02 dot1x-user username Cisco123 password Cisco2020
```

次に、アクセス ポイント cisco_ap1 の認証を無効にする例を示します。

```
Device# ap name cisco_ap1 no dot1x-user
```

ap name ethernet

Cisco Lightweight アクセス ポイントのイーサネット ポート設定を指定するには、**apnameethernet** コマンドを使用します。指定されたポート設定またはデフォルトの設定を削除には、このコマンドの **no** 形式を使用します。

ap name *ap-name* **ethernet** *intf-number* **mode** {**access** *vlan-id*| **trunk** [**add**| **delete**]} **native-vlan** *vlan-id*

ap name *ap-name* **no ethernet** *intf-number* **mode** {**access**| **trunk native-vlan**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
intf-number	イーサネット インターフェイス番号（0 ～ 3）。
mode	アクセス モードまたはトランク モードを設定します。
access	アクセス モードでポートを設定します。
vlan-id	VLAN 識別番号。
trunk	トランク モードでポートを指定します。
add	（任意）VLAN モードまたはトランク モードを追加します。
delete	（任意）VLAN モードまたはトランク モードを削除します。
native-vlan	ネイティブ VLAN を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、シスコのアクセス ポイントのアクセス モードを設定する例を示します。

```
Device# ap name AP2 ethernet 0 mode access 1
```

ap name ethernet duplex

Lightweightアクセス ポイントのイーサネット ポート デュプレックスおよび速度を設定するには、**apnameethernetduplex** コマンドを使用します。

ap name *ap-name* **ethernet duplex** {**auto**| **full**| **half**} **speed**{**10**| **100**| **1000**| **auto**}

構文の説明

ap-name	Cisco アクセス ポイントの名前。
auto	イーサネット ポートの自動二重設定を指定します。
full	イーサネット ポートの全二重設定を指定します。
half	イーサネット ポートの半二重設定を指定します。
speed	イーサネット ポート速度の設定を指定します。
10	イーサネット ポート速度を 10 Mbps に指定します。
100	イーサネット ポート速度を 100 Mbps に指定します。
1000	イーサネット ポート速度を 1000 Mbps に指定します。
auto	接続されているすべてのアクセス ポイントにイーサネット ポートの設定を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセスポイントのイーサネットポートを全二重および1 Gbpsに設定する例を示します。

```
Device# ap name AP2 ethernet duplex full 1000
```

ap name key-zeroize

アクセス ポイントで FIPS キー ゼロ化を有効にするには、**ap name<AP name>key-zeroize** コマンドを使用します。

ap name*ap-name***key-zeroize**

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
key-zeroize	アクセス ポイントに、アクセス ポイントで FIPS キー ゼロ化を有効にするように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次の例では、FIPS キー ゼロ化を有効にする方法を示します。

```
Device(config)#ap name <AP Name> key-zeroize
```

ap name image

特定のアクセス ポイントでイメージを設定するには、**apnameimage** コマンドを使用します。

ap name *ap-name* **image** {**predownload| swap**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

predownload	アクセス ポイントにイメージのプレダウンロードを開始するように指示します。
swap	アクセス ポイントにイメージを切り替えるように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントにイメージをプレダウンロードする例を示します。

```
Device# ap name AP2 image predownload
```

次に、アクセス ポイントのプライマリおよびセカンダリ イメージを切り替える例を示します。

```
Device# ap name AP2 image swap
```

ap name ipv6 tcp adjust-mss

シスコの AP の IPv6 TCP 最大セグメント サイズ（MSS）値を設定するには、**ap name ipv6 tcp adjust-mss** コマンドを使用します。

ap name *ap-name* **ipv6 tcp adjust-mss** *size*

ap name *ap-name* **no ipv6 tcp adjust-mss**

構文の説明

ap-name	Cisco AP の名前。
adjust-mss	すべてのシスコ AP の IPv6 TCP MSS を設定します。
size	MSS 値（500 ～ 1440）。

コマンド デフォルト

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

MSS 値は 500 ～ 1440 の範囲でなければなりません。

次に、シスコのアクセス ポイント AP01 の IPv6 TCP MSS 値を 600 に設定する例を示します。

```
Device# ap name AP01 ipv6 tcp adjust-mss 600
```

ap name jumbo mtu

ジャンボ MTU サポートを設定するには、**ap name<AP name>jumbo-mtu** コマンドを使用します。

ap name*ap-name*{**jumbo-mtu**| **no jumbo-mtu**}

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
jumbo-mtu	アクセス ポイントに ジャンボ MTU サポートを有効にするように指示します。
no jumbo-mtu	アクセス ポイントに ジャンボ MTU サポートを無効にするように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、ジャンボ MTU サポートを設定する例を示します。

```
Deviceap name <AP Name> jumbo-mtu
```

ap name lan

AP の LAN ポート設定を指定するには、**ap name lan** コマンドを使用します。AP の LAN ポート設定を削除するには、**ap name no lan** コマンドを使用します。

ap name *ap-name* **[no]lan port-id** *port-id* {**shutdown**|**vlan-access**}

構文の説明

no	LANポート設定を削除します。
port-id	ポートを設定します。
port-id	ポートの ID。範囲は 1 ～ 4 です。
shotdown	ポートを無効にします。
vlan-access	ポートへの VLAN アクセスを有効にします。

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
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、ポートへの VLAN アクセスを有効にする例を示します。

```
Device# ap name AP1 lan port-id 1 vlan-access
```

ap name led

アクセス ポイントのLEDステートを有効にするには、**apnameled**コマンドを使用します。アクセス ポイントの LED ステートを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **led**

no ap name *ap-name* [**led**] **led**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
led	アクセス ポイントの LED ステートを有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの LED ステートを有効にする例を示します。

```
Device# ap name AP2 led
```

次に、アクセス ポイントの LED ステートを無効にする例を示します。

```
Device# ap name AP2 no led
```

ap name link-encryption

特定の Cisco Lightweight アクセス ポイントの Datagram Transport Layer Security（DTLS）データ暗号化を有効にするには、**apname link-encryption** コマンドを使用します。Cisco Lightweight アクセス ポイントの DTLS データ暗号化を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **link-encryption**

ap name *ap-name* **no link-encryption**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントのデータ暗号化を有効にする例を示します。

```
Device# ap name AP02 link-encryption
```

ap name link-latency

デバイス に現在関連付けられている特定の Cisco Lightweight アクセス ポイントのリンク遅延を有効にするには、**apnamelink-latency** コマンドを使用します。デバイス に現在関連付けられている特定の Cisco Lightweight アクセス ポイントのリンク遅延を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **link-latency**

ap name *ap-name* **no link-latency**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

リンク遅延は、デフォルトでは無効になります。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、現在デバイスに参加しているアクセス ポイントだけに対してリンク遅延を有効または無効にします。将来参加するアクセス ポイントには適用されません。

次に、アクセス ポイントでリンク遅延を有効にする例を示します。

```
Device# ap name AP2 link-latency
```

ap name location

Cisco Lightweight アクセス ポイントのロケーション説明を変更するには、**apnamelocation** コマンドを使用します。

ap name *ap-name* **location** *location*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
location	アクセス ポイントのロケーション名（二重引用符で囲みます）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

Cisco Lightweight アクセス ポイントを無効にしてから、このパラメータを変更する必要があります。

次に、アクセス ポイント AP1 のロケーションの説明を設定する例を示します。

```
Device# ap name AP1 location Building1
```

ap name mgmtuser

アクセス ポイント管理用のユーザ名、パスワード、シークレット パスワードを設定するには、**apnamemgmtuser** コマンドを使用します。特定のアクセス ポイントがデバイスのグローバル クレデンシャルを強制的に使用するには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **mgmtuser username** *username* **password** *password* **secret** *secret*

ap name *ap-name* **no mgmtuser**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
username	アクセス ポイント管理用のユーザ名を指定します。
username	管理ユーザ名。
password	アクセス ポイント管理用のパスワードを指定します。
password	アクセス ポイント管理パスワード。
secret	特権アクセス ポイント管理用のシークレット パスワードを指定します。
secret	アクセス ポイント管理シークレット パスワード。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

強力なパスワードを指定するには、次の要件を満たす必要があります。

- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。
- パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
- パスワードに管理ユーザ名や逆にしたユーザ名を含めることはできません。
- パスワードに使用できない文字には、Cisco、oscic、admin、nimda などの語のほか、大文字の代わりに 1 や|、! を、o の代わりに 0 を、s の代わりに $ を使用して置き換えた文字などがあります。

シークレット パスワードについて、次の要件が実施されます。

- シークレット パスワードは、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスを含むことができません。

次に、アクセスポイント管理用のユーザ名、パスワード、シークレットパスワードを追加する例を示します。

```
Device# ap name AP01 mgmtuser username acd password Arc_1234 secret Mid_1234
```

ap name mode

個別の Cisco Lightweight アクセス ポイントの Cisco デバイス 通信オプションを変更するには、**apnamemode** コマンドを使用します。

ap name *ap-name* **mode**{**local submode**{**none**| **wips**}| **monitor submode**{**none**| **wips**}| **rogue**| **se-connect**| **sniffer**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
local	屋内メッシュ アクセス ポイント（MAP または RAP）から nonmesh Lightweight アクセス ポイント（ローカル モード）に変換します。

submode	アクセス ポイントで wIPS サブモードを指定します。
none	アクセス ポイントで wIPS を無効にします。
monitor	監視モードの設定を指定します。
wips	アクセス ポイントで wIPS サブモードを有効にします。
rogue	アクセス ポイントで有線の不正なアクセス ポイントの検出モードを有効にします。
se-connect	アクセス ポイントで Spectrum Expert モードを有効にします。
sniffer	アクセス ポイントで無線スニファ モードを有効にします。

コマンド デフォルト

ローカル

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

スニファ モードは、そのチャネル上のクライアントからすべてのパケットを取得し、Airopeek を実行するリモート マシンまたはその他のサポート対象パケット アナライザ ソフトウェアに転送します。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

次に、ローカル モードでアクセス ポイント AP01 と通信するようにデバイスを設定する例を示します。

```
Device# ap name AP01 mode local submode none
```

次に、有線の不正なアクセス ポイントの検出モードでアクセス ポイント AP01 と通信するようにデバイスを設定する例を示します。

```
Device# ap name AP01 mode rogue
```

次に、無線スニファ モードでアクセス ポイント AP02 と通信するようにデバイスを設定する例を示します。

```
Device# ap name AP02 mode sniffer
```

ap name monitor-mode

Cisco Lightweight アクセス ポイント チャネルの最適化を設定するには、**apnamemonitor-mode** コマンドを使用します。

ap name *ap-name* **monitor-mode** {**no-optimization| tracking-opt| wips-optimized**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
no-optimization	アクセス ポイントに対してチャネル スキャンの最適化を行わないことを指定します。
tracking-opt	アクセス ポイントに対してトラッキングが最適化されたチャネル スキャンを有効にします。
wips-optimized	アクセス ポイントに対して wIPS が最適化されたチャネル スキャンを有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント AP01 に Cisco wireless Intrusion Prevention System（wIPS）監視モードを設定する例を示します。

```
Device# ap name AP01 monitor-mode wips
```

ap name monitor-mode dot11b

監視モード アクセス ポイントに対して 802.11b スキャン チャネルを設定するには、**apnamemonitor-modedot11b** コマンドを使用します。

ap name *ap-name* **monitor-mode dot11b fast-channel** *channel1* [*channel2*] [*channel3*] [*channel4*]

構文の説明

ap-name	アクセス ポイントの名前。
fast-channel	監視モード アクセス ポイントに対して 2.4 GHz 帯域スキャン チャネル（単一または複数）を指定します。
channel1	channel1 のスキャン。
channel2	（任意）channel2 のスキャン。
channel3	（任意）channel3 のスキャン。
channel4	（任意）channel4 のスキャン。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、チャネル1、6、11をリッスンするようにトラッキング最適化モードのアクセスポイントを設定する例を示します。

```
Device# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

ap name name

Cisco Lightweight アクセス ポイントの名前を変更するには、**apnamename** コマンドを使用します。

ap name *ap-name* **name** *new-name*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの現在の名前。
new-name	Cisco Lightweight アクセス ポイントの新しい名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの名前を AP1 から AP2 に変更する例を示します。

```
Device# ap name AP1 name AP2
```

ap name no dot11 shutdown

802.11 ネットワーク上の個別のシスコ無線の無線伝送を有効にするには、**apnamenodot11shutdown** コマンドを使用します。

ap name *ap-name* **no dot11** {**24ghz**| **5ghz**} **shutdown**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 無線を指定します。

5ghz	5 GHz 無線を指定します。

コマンド デフォルト

デフォルトでは、ネットワーク全体で伝送が有効化されています。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

（注） 802.11 を設定する場合は、このコマンドを **apname***Cisco-AP***dot115ghzshutdown** コマンドとともに使用します。

このコマンドは、CLI インターフェイスがアクティブなときはいつでも使用できます。

次に、アクセス ポイント AP1 の 5 GHz 帯域での無線伝送を有効にする例を示します。

```
Device# ap name AP1 no dot11 5ghz shutdown
```

ap name power

アクセス ポイントの Cisco Power over Ethernet（PoE）機能を有効にするには、**apnamepower** コマンドを使用します。アクセス ポイントの Cisco PoE 機能を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **power** {**injector| pre-standard**}

ap name *ap-name* **no power** {**injector| pre-standard**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
injector	アクセス ポイントのパワー インジェクタ ステートを指定します。

pre-standard	アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントのパワー インジェクタ ステートを有効にする例を示します。

```
Device# ap name AP01 power injector
```

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にする例を示します。

```
Device# ap name AP02 power pre-standard
```

ap name shutdown

特定の Cisco Lightweight アクセス ポイントを無効にするには、**apnameshutdown** コマンドを使用します。Cisco Lightweight アクセス ポイントを有効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **shutdown**

ap name *ap-name* **no shutdown**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、特定の Cisco Lightweight アクセス ポイントを無効にする例を示します。

```
Device# ap name AP2 shutdown
```

ap name slot shutdown

特定の Cisco Lightweight アクセス ポイントでスロットを無効にするには、**apnameslotshutdown** コマンドを使用します。Cisco Lightweight アクセス ポイントでスロットを有効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **slot** {**0**| **1**| **2**| **3**} **shutdown**

ap name *ap-name* **no slot** {**0**| **1**| **2**| **3**} **shutdown**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
0	Cisco Lightweight アクセス ポイントでスロット番号 0 を有効にします。
1	Cisco Lightweight アクセス ポイントでスロット番号 1 を有効にします。
2	Cisco Lightweight アクセス ポイントでスロット番号 2 を有効にします。
3	Cisco Lightweight アクセス ポイントでスロット番号 3 を有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、TSIM_AP2 というシスコのアクセス ポイントでスロット 0 を有効にする例を示します。

```
Device# ap name TSIM_AP2 no slot 0 shutdown
```

ap name sniff

アクセス ポイントでスニフィングを有効にするには、**apname sniff** コマンドを使用します。アクセス ポイントでスニフィングを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **sniff** {**dot11a**| **dot11b**}

ap name *ap-name* **no sniff** {**dot11a**| **dot11b**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
dot11a	2.4 GHz 帯域を指定します。
dot11b	5 GHz 帯域を指定します。
channel	スニファされる有効なチャネル。5 GHz 帯域の場合、範囲は 36 ～ 165 です。2.4 GHz 帯域の場合、範囲は 1 ～ 14 です。
server-ip-address	Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレス。

コマンド デフォルト

チャネル 36

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

アクセスポイントでスニフィング機能が有効になっている場合、そのアクセスポイントは指定されたチャネルで信号のスニフィングを開始します。すべてのパケットが取得され、Omnipeek、Airopeek、AirMagnet、または Wireshark ソフトウェアを実行しているリモート コンピュータに転送されます。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

アクセスポイントをスニファとして機能させるには、そのアクセスポイントが送信したパケットを、上記いずれかのパケットアナライザを実行しているリモートコンピュータが受信できるように設定しておく必要があります。

次に、プライマリ無線 LAN コントローラ上のアクセス ポイントの 5 GHz 帯域でのスニフィングを有効にする例を示します。

```
Device# ap name AP2 sniff dot11a 36 192.0.2.54
```

ap name ssh

特定の Cisco Lightweight アクセス ポイントでセキュア シェル（SSH）接続を有効にするには、**apnamessh** コマンドを使用します。特定の Cisco Lightweight アクセス ポイントで SSH 接続を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **ssh**

ap name *ap-name* **no ssh**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

Cisco デバイスは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco ワイヤレス LAN コントローラと関連付けられます。

次に、アクセス ポイント Cisco_ap2 で SSH 接続を有効にする例を示します。

```
Device# ap name Cisco_ap2 ssh
```

ap name telnet

アクセス ポイントで Telnet 接続を有効にするには、**apnametelnet** コマンドを使用します。アクセス ポイントで Telnet 接続を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **telnet**

ap name *ap-name* **no telnet**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント cisco_ap1 で Telnet 接続を無効にする例を示します。

```
Device# ap name cisco_ap1 no telnet
```

ap name power injector

アクセス ポイントのパワー インジェクタ ステートを設定するには、**apnamepowerinjector** コマンドを使用します。アクセス ポイントの Cisco Power over Ethernet（PoE）機能を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **power injector** {**installed| override| switch-mac-address** *switch-MAC-address*}

ap name *ap-name* **no power injector**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
installed	パワー インジェクタが設置された現在のスイッチ ポートの MAC アドレスを検出します。
override	安全性チェックを上書きし、パワーインジェクタが常にインストールされていることを前提とします。
switch-mac-address	パワー インジェクタが設置されたスイッチ ポートの MAC アドレスを指定します。
switch-MAC-address	パワーインジェクタが設置されたスイッチポートのMACアドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントのパワー インジェクタ ステートを有効にする例を示します。

```
Device# ap name AP01 power injector switch-mac-address aaaa.bbbb.cccc
```

ap name power pre-standard

アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にするには、**apnamepowerpre-standard** コマンドを使用します。アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **power pre-standard**

ap name *ap-name* **no power pre-standard**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にする例を示します。

```
Device# ap name AP02 power pre-standard
```

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを無効にする例を示します。

```
Device# ap name AP02 no power pre-standard
```

ap name reset-button

アクセス ポイントの Reset ボタンを設定するには、**apnamereset-button** コマンドを使用します。

構文の説明

ap name *ap-name* **reset-button**

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント AP03 のリセット ボタンを有効にする例を示します。

```
Device# ap name AP03 reset-button
```

ap name reset

特定の Cisco Lightweight アクセス ポイントをリセットするには、**apnamereset** コマンドを使用します。

ap name *ap-name* **reset**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、AP2 という Cisco Lightweight アクセス ポイントをリセットする例を示します。

```
Device# ap name AP2 reset
```

ap name slot

さまざまなスロット パラメータを設定するには、**apnameslot** コマンドを使用します。Cisco Lightweight アクセス ポイントでスロットを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **slot** *slot-number* {**channel** {**global**| **number** *channel-number*| **width** *channel-width*}| **rtsthreshold** *value*| **shutdown**| **txpower** {**global**| *channel-level*}}

ap name *ap-name* **no slot** {**0**| **1**| **2**| **3**} **shutdown**

構文の説明

ap-name	Cisco アクセス ポイントの名前。
slot-number	チャネルが割り当てられたスロットのダウンリンク無線。次のスロット番号を指定できます。 • **0**：Cisco Lightweight アクセス ポイントでスロット番号 0 を有効にします。 • **1**：Cisco Lightweight アクセス ポイントでスロット番号 1 を有効にします。 • **2**：Cisco Lightweight アクセス ポイントでスロット番号 2 を有効にします。 • **3**：Cisco Lightweight アクセス ポイントでスロット番号 3 を有効にします。
channel	スロットのチャネルを指定します。
global	スロットのチャネル グローバル プロパティを指定します。
number	スロットのチャネル番号を指定します。
channel-number	チャネル番号（1 ～ 169）。
width	スロットのチャネル幅を指定します。
channel-width	チャネル幅（20 ～ 40）。
rtsthreshold	アクセス ポイントの RTS/CTS しきい値を指定します。

value	RTS/CTS しきい値（0 ～ 65535）。
shutdown	スロットをシャット ダウンします。
txpower	スロットの Tx 電力を指定します。
global	スロットの自動-RF を指定します。
channel-level	スロットの送信電力レベル（1 ~ 7）電源レベル。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント abc のスロット 3 を有効にする例を示します。

```
Device# ap name abc slot 3
```

次に、アクセス ポイント abc の RTS を設定する例を示します。

```
Device# ap name abc slot 3 rtsthreshold 54
```

ap name static-ip

Cisco Lightweight アクセス ポイントの静的 IP アドレス設定を指定するには、**apnamestatic-ip** コマンドを使用します。Cisco Lightweight アクセス ポイントの静的 IP アドレスを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **static-ip** {**domain** *domain-name*| **ip-address** *ip-address* **netmask** *netmask* **gateway** *gateway*| **nameserver** *ip-address*}

ap name *ap-name* **no static-ip**

構文の説明

ap-name	アクセス ポイントの名前。

domain	シスコのアクセス ポイントのドメイン名を指定します。
domain-name	特定のアクセス ポイントが属するドメイン。
ip-address	シスコのアクセス ポイントの静的 IP アドレスを指定します。
ip-address	シスコのアクセス ポイントの静的 IP アドレス。
netmask	シスコのアクセス ポイントの静的 IP ネットマスクを指定します。
netmask	シスコのアクセス ポイントの静的 IP ネットマスク。
gateway	シスコのアクセス ポイントのゲートウェイを指定します。
gateway	シスコのアクセス ポイントのゲートウェイの IP アドレス。
nameserver	特定のアクセス ポイントが DNS 解決を使用してデバイスを検出できるよう DNS サーバを指定します。
ip-address	DNS サーバの IP アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバと、アクセス ポイントが属するドメインとを指定しない限り、アクセス ポイントはドメイン ネーム システム（DNS）解決を使用してデバイスを検出できません。

次に、アクセス ポイントの静的 IP アドレスを設定する例を示します。

```
Device# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway 192.0.2.1
```

ap name stats-timer

Cisco Lightweight アクセス ポイントがその DOT11 統計情報を Cisco デバイスに送信する時間（秒単位）を設定するには、**apnamestats-timer** コマンドを使用します。

ap name *ap-name* **stats-timer** *timer-value*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
timer-value	0 ～ 65535 の時間（秒単位）。ゼロの値を指定すると、タイマーが無効になります。

コマンド デフォルト

0（無効）。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

値 0 は、Cisco Lightweight アクセス ポイントが DOT11 統計情報を送信しないことを意味します。このタイマーには 0 ～ 65,535 秒を指定できます。Cisco Lightweight アクセス ポイントを無効にしてから、この値を設定する必要があります。

次に、アクセス ポイント AP2 で、統計情報タイマーを 600 秒に設定する例を示します。

```
Device# ap name AP2 stats-timer 600
```

ap name syslog host

特定の Cisco Lightweight アクセス ポイントの syslog サーバを設定するには、**apnamesysloghost** コマンドを使用します。

ap name *ap-name* **syslog host** *syslog-host-ip-address*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
syslog-host-ip-address	syslog サーバの IP アドレス。

コマンド デフォルト

255.255.255.255

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、各アクセス ポイントの syslog サーバ IP アドレスは 255.255.255.255 で、これはまだサーバが設定されていないことを示しています。このデフォルト値を使用すると、グローバル アクセス ポイント syslog サーバの IP アドレスがアクセス ポイントにプッシュされます。

次に、syslog サーバを設定する例を示します。

```
Device# ap name AP2 syslog host 192.0.2.54
```

ap name syslog level

システム ログ レベルを設定するには、**apnamesysloglevel** コマンドを使用します。

ap name *ap-name* **syslog level** {**alert| critical| debug| emergency| errors| information| notification| warning**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
alert	アラート レベルのシステム ログを指定します。

critical	クリティカル レベルのシステム ログを指定します。
debug	デバッグ レベルのシステム ログを指定します。
emergency	緊急レベルのシステム ログを指定します。
errors	エラー レベルのシステム ログを指定します。
information	情報レベルのシステム ログを指定します。
notification	通知レベルのシステム ログを指定します。
warning	警告レベルのシステム ログを指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アラート レベルのシステム ログを設定する例を示します。

```
Device# ap name AP2 syslog level alert
```

ap name tcp-adjust-mss

特定のアクセス ポイントで TCP 最大セグメント サイズ（MSS）を有効または無効にするには、**apnametcp-adjust-mss** コマンドを使用します。特定のアクセス ポイントで TCP 最大セグメント サイズ（MSS）を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **tcp-adjust-mss size** *size*

ap name *ap-name* **no tcp-adjust-mss**

構文の説明

ap-name	アクセス ポイントの名前。

size	最大セグメント サイズ（536 ～ 1363 バイト）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

この機能を有効にすると、アクセス ポイントがデータ パスの無線クライアントへの TCP パケットとデータ パスの無線クライアントからの TCP パケットをチェックします。これらのパケットの MSS が設定した値または Control And Provisioning of Wireless Access Points（CAPWAP）トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。これらのパケットの MSS が設定した値または CAPWAP トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、新しく設定された値に変更します。

次に、アクセス ポイント Cisco_ap1 で TCP MSS を有効にする例を示します。

```
Device# ap name ciscoap tcp-adjust-mss size 1200
```

ap name tftp-downgrade

Lightweight アクセス ポイントを Autonomous アクセス ポイントにダウングレードするために使用される設定を指定するには、**apnametftp-downgrade** コマンドを使用します。

ap name *ap-name* **tftp-downgrade** *tftp-server-ip filename*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
tftp-server-ip	TFTP サーバの IP アドレス。
filename	TFTP サーバ上のアクセス ポイント イメージ ファイルのファイル名。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント AP1 をダウングレードする設定を指定する例を示します。

```
Device# ap name Ap01 tftp-downgrade 172.21.12.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

ap power injector

デバイス に参加しているすべての Cisco Lightweight アクセス ポイントのパワー インジェクタ ステートを設定するには、**appowerinjector** コマンドを使用します。すべてのアクセス ポイントのパワー インジェクタ ステ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。

ap power injector {**installed**| **override**| **switch-mac-address** *switch-MAC-addr*}

no ap power injector

構文の説明

installed	パワー インジェクタが設置された現在のスイッチ ポートの MAC アドレスを検出します。
override	安全性チェックを上書きし、パワーインジェクタが常にインストールされていることを前提とします。
switch-mac-address	パワーインジェクタが設置されたスイッチ ポートの MAC アドレスを指定します。
switch-MAC-address	パワーインジェクタが設置されたスイッチ ポートの MAC アドレスを指定します。

コマンド デフォルト

なし グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、デバイスに参加しているすべての Cisco Lightweight アクセス ポイントのパワー インジェクタ ステートを有効にする例を示します。

```
Device(config)# ap power injector switch-mac-address aaaa.bbbb.cccc
```

ap power pre-standard

デバイスに参加している Cisco Lightweight アクセス ポイントを、シスコのハイパワー スイッチによって電力が供給されるように設定するには、**appowerpre-standard** コマンドを使用します。すべてのアクセス ポイントの先行標準電力を無効にするには、このコマンドの **no** 形式を使用します。

ap power pre-standard

no ap power pre-standard

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にする例を示します。

```
Controller(config)# ap power pre-standard
```

ap reporting-period

アクセス ポイント不正/エラー レポート期間を設定するには、**apreporting-period** コマンドを使用します。アクセス ポイント不正/エラー レポート期間を無効にするには、このコマンドの **no** 形式を使用します。

ap reporting-period *value*

no ap reporting-period

構文の説明

value	秒単位の期間（10 ～ 120）。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント不正/エラー レポートを設定する例を示します。

```
Device(config)# ap reporting-period 100
```

次に、アクセス ポイント不正/エラー レポートを無効にする例を示します。

```
Device(config)# no ap reporting-period 100
```

ap reset-button

デバイス に参加しているすべての Cisco Lightweight アクセス ポイントの Reset ボタンを設定するには、**apreset-button** コマンドを使用します。すべてのアクセス ポイントの Reset ボタンを無効にするには、このコマンドの **no** 形式を使用します。

ap reset-button

no ap reset-button

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、コントローラに参加しているすべてのアクセス ポイントの Reset ボタンを設定する例を示します。

```
Device(config)# ap reset-button
```

service-policy type control subscriber

グローバル サブスクライバ制御ポリシーを適用するには、 **service-policy type control subscriber** <*subscriber-policy-name*> コマンドを使用します。

service-policytypecontrolsubscriber<*subscriber-policy-name*>

構文の説明

service-policy	アクセスポイントにグローバルサブスクライバ制御ポリシーを適用するように指示します。
<*subscriber-policy-name*>	サブスクライバ ポリシーの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、グローバル サブスクライバ制御ポリシーを無効にする例を示します。

```
Deviceno service-policy type control subscriber
```

ap static-ip

Cisco Lightweight アクセス ポイントの静的 IP アドレスを設定するには、**apstatic-ip** コマンドを使用します。アクセス ポイントの静的 IP 設定を無効にするには、このコマンドの **no** 形式を使用します。

ap static-ip {**domain** *domain-name*| **name-server** *ip-address*}

no ap static-ip {**domain**| **name-server**}

構文の説明

domain	特定のアクセスポイントまたはすべてのアクセスポイントが属するドメインを指定します。
domain-name	ドメイン名。
name-server	特定のアクセス ポイントまたはすべてのアクセス ポイントが DNS 解決を使用してデバイスを検出できるよう DNS サーバを指定します。
ip-address	DNS サーバの IP アドレス。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバと、アクセス ポイントが属するドメインとを指定しない限り、アクセス ポイントはドメイン ネーム システム（DNS）解決を使用してデバイスを検出できません。

次に、すべてのアクセス ポイントの静的 IP アドレスを設定する例を示します。

```
Device(config)# ap static-ip domain cisco.com
```

ap syslog

デバイスに参加しているすべての Cisco Lightweight アクセス ポイントのシステム ログを設定するには、**apsyslog** コマンドを使用します。

ap syslog {**host** *ipaddress*| **level**{**alert**| **critical**| **debug**| **emergency**| **errors**| **information**| **notification**| **warning**}}

構文の説明

host	デバイスに参加しているすべてのアクセス ポイントのグローバル syslog サーバを指定します。
ipaddress	syslog サーバの IP アドレス。
level	デバイスに参加しているすべてのアクセス ポイントのシステム ログ レベルを指定します。
alert	シスコのアクセス ポイントのアラート レベルのシステム ログを指定します。
critical	シスコのアクセス ポイントのクリティカル レベルのシステム ログを指定します。
debug	シスコのアクセス ポイントのデバッグ レベルのシステム ログを指定します。
emergency	シスコのアクセス ポイントの緊急レベルのシステム ログを指定します。

errors	シスコのアクセス ポイントのエラー レベルのシステム ログを指定します。
information	シスコのアクセス ポイントの情報レベルのシステム ログを指定します。
notification	シスコのアクセス ポイントの通知レベルのシステム ログを指定します。
warning	シスコのアクセス ポイントの警告レベルのシステム ログを指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、すべてのアクセス ポイントのグローバル syslog サーバ IP アドレスは 255.255.255.255 です。デバイス上の syslog サーバを設定する前に、アクセス ポイントがこのサーバが常駐するサブネットにアクセスできることを確認します。このサブネットにアクセスできない場合、アクセス ポイントは syslog メッセージを送信できません。

次に、すべてのアクセス ポイントにグローバル syslog サーバを設定する例を示します。

```
Device(config)# ap syslog host 172.21.34.45
```

ap name no controller

設定済みのプライマリ、セカンダリ、およびターシャリ ワイヤレス LAN コントローラの順序を変更するには、次のコマンドを使用します。

ap name*ap-name* **no controller primary**

ap name*ap-name* **no controller secondary**

ap name*ap-name* **no controller tertiary**

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
no controller primary	アクセス ポイントにプライマリ コントローラの構成解除を指示します。
no controller secondary	アクセス ポイントにセカンダリ コントローラの構成解除を指示します。
no controller tertiary	アクセス ポイントにターシャリ コントローラの構成解除を指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

アクセスポイントに対して設定されているプライマリ、セカンダリ、およびターシャリ ワイヤレス LAN コントローラがあり、コントローラの名前と対応する IP アドレスを交換する必要がある場合、プライマリ コントローラを構成解除して、セカンダリ コントローラを構成できます。

例

次に、プライマリ コントローラを構成解除する例を示します。

```
Deviceap name <AP Name> no controller primary.
```

ap tcp-adjust-mss size

すべての Cisco Lightweight アクセス ポイントで TCP 最大セグメント サイズ（MSS）を有効にするには、**aptcp-adjust-msssize** コマンドを使用します。すべての Cisco Lightweight アクセス ポイン

トで TCP 最大セグメント サイズ（MSS）を無効にするには、このコマンドの **no** 形式を使用します。

ap tcp-adjust-mss size *size*

no ap tcp-adjust-mss

構文の説明

size	最大セグメント サイズ（536 ～ 1363 バイト）。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

この機能を有効にすると、アクセス ポイントがデータ パスの無線クライアントへの TCP パケットとデータ パスの無線クライアントからの TCP パケットをチェックします。これらのパケットの MSS が設定した値または Control And Provisioning of Wireless Access Points（CAPWAP）トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。

次に、セグメント サイズが 1200 のすべてのアクセス ポイントで TCP MSS を有効にする例を示します。

```
Device(config)# ap tcp-adjust-mss 1200
```

ap tftp-downgrade

Lightweight アクセス ポイントを Autonomous アクセス ポイントにダウングレードするために使用される設定を指定するには、**aptftp-downgrade** コマンドを使用します。Lightweight アクセス ポイントを Autonomous アクセス ポイントにダウングレードするために使用される設定を無効にするには、このコマンドの **no** 形式を使用します。

ap tftp-downgrade *tftp-server-ip filename*

no ap tftp-downgrade

構文の説明

tftp-server-ip	TFTP サーバの IP アドレスです。
filename	TFTP サーバ上のアクセス ポイント イメージ ファイルのファイル名。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントをダウングレードする設定を指定する例を示します。

```
Device(config)# ap tftp-downgrade 172.21.23.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

config wireless wps rogue client mse

不正 MSE クライアントを設定するには、**wirelesswps rogueclientmse** コマンドを使用します。

ワイヤレス クライアントの統計情報の概要を表示するには、**showwirelessclientclient-statisticssummary** コマンドを使用します。

wirelesswpsrogueclientmse

showwirelessclientclient-statisticssummary

構文の説明

rogueclientmse	不正MSEクライアントの設定を有効にするようアクセスポイントに命令します。

nowirelesswps	不正MSEクライアントの設定を無効にするようアクセスポイントに命令します。
client-statisticssummary	ワイヤレス クライアントの統計情報の概要を表示するよう命令します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、不正 MSE クライアントを設定する例を示します。

```
Device(config)#wireless wps rogue client mse
```

clear ap name tsm dot11 all

特定のアクセス ポイントまたはすべてのアクセス ポイントのトラフィック ストリーム メトリック（TSM）統計情報をクリアするには、**clearapnametsmdot11all** コマンドを使用します。

clear ap name *ap-name* **tsm dot11** {**24ghz**| **5ghz**} **all**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
all	すべてのアクセス ポイントを指定します。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz 帯域のアクセス ポイントの TSM 統計情報をクリアする例を示します。

```
Device# clear ap name AP1 tsm dot11 24ghz all
```

clear ap config

Lightweight アクセス ポイントの設定をクリア（デフォルト値にリセット）するには、**clearapconfig** コマンドを使用します。

clear ap config *ap-name* [**eventlog**| **keep-ip-config**]

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
eventlog	（任意）デバイスに参加している特定のアクセスポイントまたはすべてのアクセス ポイントの既存のイベント ログ ファイルを削除して空のイベント ログ ファイルを作成します。
keep-ip-config	（任意）シスコのアクセス ポイントの静的 IP 設定を削除しないように指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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ても、アクセス ポイントの固定 IP アドレスはクリアされません。

次に、AP01 という名前のアクセス ポイント用のアクセス ポイントの設定をクリアする例を示します。

```
Device# clear ap config AP01
```

clear ap eventlog-all

すべてのアクセス ポイントの既存のイベント ログを削除して空のイベント ログ ファイルを作成するには、**clearapeventlog-all** コマンドを使用します。

clear ap eventlog-all

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントのイベント ログを削除する例を示します。

```
Device# clear ap eventlog-all
```

clear ap join statistics

すべてのアクセス ポイントまたは特定のアクセス ポイントの参加統計情報をクリアするには、**clearapjoinstatistics** コマンドを使用します。

clear ap join statistics

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントの参加統計情報をクリアする例を示します。

```
Device# clear ap join statistics
```

clear ap mac-address

特定の Cisco Lightweight アクセス ポイントの参加統計情報の MAC アドレスをクリアするには、**clearapmac-address** コマンドを使用します。

clear ap mac-address *mac* **join statistics**

構文の説明

mac	アクセス ポイントの MAC アドレス。
joinstatistics	参加統計情報をクリックします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの参加統計情報をクリアする例を示します。

```
Device# clear ap mac-address aaaa.bbbb.cccc join statistics
```

clear ap name wlan statistics

WLAN 統計情報をクリアするには、**clearapnamewlanstatistics** コマンドを使用します。

clear ap name *ap-name* **wlan statistics**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント cisco_ap の WLAN 設定要素をクリアする例を示します。

```
Device# clear ap name cisco_ap wlan statistics
```

debug ap mac-address

MAC-アドレス上のアクセス ポイントのデバッグを有効にするには、**debugapmac-address** コマンドを使用します。

debug ap mac-address *mac-address*

no debug ap mac-address *mac-address*

構文の説明

mac-address	アクセス ポイント Ethernet MAC アドレス、または 802.11 無線インターフェイスの MAC アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
10.3Cisco IOS XE 3.3 SE	このコマンドが導入されました。

次に、AP での MAC アドレスのデバッグを有効にする例を示します。

```
Device# debug ap mac-address
ap mac-address debugging is on
```

次に、AP での MAC アドレスのデバッグを無効にする例を示します。

```
Device# no debug ap mac-address
ap mac-address debugging is off
```

show ap cac voice

使用されている帯域幅、使用可能な最大帯域幅、コール情報を含む簡潔な音声統計とともにすべてのアクセス ポイントの一覧を表示するには、**showapcacvoice** コマンドを使用します。

show ap cac voice

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、Cisco Lightweight アクセス ポイントに対応する音声 CAC の詳細を表示する例を示します。

```
controller# show ap cac voice

1) AP Name: AP01
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ------------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
  3    1      1        maria-open            0           0
  4    1      12       24                    0           0


2) AP Name: AP02
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ------------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
  3    1      1        maria-open            0           0
  4    1      12       24                    0           0
```

show ap capwap

すべてのアクセス ポイントに適用される Control And Provisioning of Wireless Access Points（CAPWAP）設定を表示するには、**showapcapwap** コマンドを使用します。

show ap capwap {**retransmit| timers| summary**}

構文の説明

retransmit	アクセス ポイント CAPWAP 再送信パラメータを表示します。
timers	不正アクセス ポイント エントリ タイマーを表示します。
summary	シスコ デバイスのネットワーク設定を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント CAPWAP 再送信パラメータを表示する例を示します。

```
Controller# show ap capwap retransmit

Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval           Retransmit Count
-----------------------------------------------------------------------------------
AP01                              3                             5

AP02                              3                             5

AP03                              3                             5

AP04                              3                             5

AP05                              3                             5

AP07                              3                             5

AP08                              3                             5
```

```
AP09                            3                               5

AP10                            3                               5

AP11                            3                               5

AP12                            3                               5
```

次に、不正アクセス ポイント エントリ タイマーを表示する例を示します。

```
Controller# show ap capwap timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
```

次に、シスコ デバイスのネットワーク設定を表示する例を示します。

```
Controller# show ap capwap summary

AP Fallback                     : Enabled
AP Join Priority                : Disabled
AP Master                       : Disabled
Primary backup Controller Name  :
Primary backup Controller IP    : 0.0.0.0
Secondary backup Controller Name :
Secondary backup Controller IP  : 0.0.0.0
```

show ap cdp

デバイス に結合されたすべての Cisco Lightweight アクセス ポイントの Cisco Discovery Protocol（CDP）情報を表示するには、**showapcdp** コマンドを使用します。

show ap cdp [**neighbors** [**detail**]]

構文の説明

ネイバー	（任意）CDP を使用してネイバーを表示します。
detail	（任意）CDP を使用している特定のアクセス ポイントのネイバーに関する詳細を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントの CDP ステータスを表示する例を示します。

```
Device# show ap cdp
```

次に、CDP を使用しているすべてのネイバーの詳細を表示する例を示します。

```
Device# show ap cdp neighbors
```

show ap config dot11

Cisco Lightweight アクセスポイントの 802.11-58G 無線の詳細な設定を表示するには、**showapconfigdot11** コマンドを使用します。

show ap config dot11 58ghz summary

構文の説明

58ghz	802.11-58G 無線を表示します。
summary	アクセスポイントの無線のサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの 802.11a-58G の詳細な設定を表示する例を示します。

```
Device# show ap config dot11 58ghz summary
```

show ap config dot11 dual-band summary

Cisco AP のデュアルバンド無線の設定のサマリーを表示するには、**show ap config dot11 dual-band summary** コマンドを使用します。

show ap config dot11 dual-band summary

構文の説明

dual-band	デュアルバンド無線を指定します。
summary	Cisco AP のデュアルバンド無線の設定のサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

show ap config fnf

すべての Cisco AP の NetFlow 入出力モニタを表示するには、**show ap config fnf** コマンドを使用します。

show ap config fnf

構文の説明

fnf	すべての Cisco AP の NetFlow 入出力モニタ。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

show ap config

デバイスに結合するすべてのアクセス ポイントの設定を表示するには、**showapconfig** コマンドを使用します。

show ap config {**ethernet**| **general**| **global**}

構文の説明

ethernet	すべての Cisco AP の VLAN タギング情報を表示します。
general	すべての Cisco AP に共通する情報を表示します。
global	すべての Cisco AP のグローバル設定を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、グローバル syslog サーバ設定を表示する例を示します。

```
Device# show ap config global

AP global system logging host                   : 255.255.255.255
```

show ap crash-file

Lightweightアクセス ポイントによって生成されたクラッシュ ファイルおよび無線コア ダンプ ファイルの両方の一覧を表示するには、**showapcrash-file** コマンドを使用します。

show ap crash-file

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントで生成されたクラッシュ ファイルを表示する例を示します。

```
Device# show ap crash-file
```

show ap data-plane

データ プレーンのステータスを表示するには、**showapdata-plane** コマンドを使用します。

show ap data-plane

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントのデータ プレーンのステータスを表示する例を示します。

```
Device# show ap data-plane
```

show ap dot11 l2roam

802.11a または 802.11b/g レイヤ 2 クライアントのローミング情報を表示するには、**showapdot11l2roam** コマンドを使用します。

show ap dot11 {**24ghz| 5ghz**} **l2roam** {**mac-address** *mac-address* **statistics| rf-param| statistics**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
mac-address*mac-address***statistics**	Cisco Lightweight アクセス ポイントの MAC アドレスを指定します。
rf-param	レイヤ 2 周波数パラメータを指定します。
statistics	レイヤ 2 クライアントのローミング統計情報を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、802.11b レイヤ 2 クライアントのローミング情報を表示する例を示します。

```
Device# show ap dot11 24ghz l2roam rf-param

L2Roam 802.11bg RF Parameters
  Config Mode           : Default
  Minimum RSSI          : -85
  Roam Hysteresis       : 2
  Scan Threshold        : -72
  Transition time       : 5
```

show ap dot11 cleanair air-quality

802.11 ネットワークの電波品質のサマリー情報および最も深刻な電波品質の情報を表示するには、**showapdot11cleanairair-quality** コマンドを使用します。

show ap dot11 {**24ghz**| **5ghz**} **cleanair air-quality** {**summary**| **worst**}

構文の説明

24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
summary	802.11 無線帯域電波品質情報のサマリーを表示します。
worst	802.11 ネットワークの最も深刻な電波品質の情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、5 GHz 帯域の最も深刻な電波品質の情報を表示する例を示します。

```
Device# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 36      95     70     0           40
```

次に、2.4 GHz 帯域の最も深刻な電波品質の情報を表示する例を示します。

```
Device# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 1       83     57     3           5
```

show ap dot11 cleanair config

802.11 ネットワークの CleanAir 設定を表示するには、**showapdot11cleanairconfig** コマンドを使用します。

show ap dot11 {**24ghz**| **5ghz**} **cleanair config**

構文の説明

24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、2.4 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Device# show ap dot11 24ghz cleanair config
Clean Air Solution..............................: Disabled
Air Quality Settings:
    Air Quality Reporting.......................: Disabled
    Air Quality Reporting Period (min)..........: 15
    Air Quality Alarms..........................: Enabled
    Air Quality Alarm Threshold.................: 10
Interference Device Settings:
    Interference Device Reporting...............: Enabled
        Bluetooth Link..........................: Enabled
        Microwave Oven..........................: Enabled
        802.11 FH...............................: Enabled
        Bluetooth Discovery.....................: Enabled
        TDD Transmitter.........................: Enabled
        Jammer..................................: Enabled
        Continuous Transmitter..................: Enabled
        DECT-like Phone.........................: Enabled
        Video Camera............................: Enabled
        802.15.4................................: Enabled
        WiFi Inverted...........................: Enabled
        WiFi Invalid Channel....................: Enabled
        SuperAG.................................: Enabled
        Canopy..................................: Enabled
        Microsoft Device........................: Enabled
        WiMax Mobile............................: Enabled
        WiMax Fixed.............................: Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link..........................: Disabled
        Microwave Oven..........................: Disabled
        802.11 FH...............................: Disabled
        Bluetooth Discovery.....................: Disabled
        TDD Transmitter.........................: Disabled
        Jammer..................................: Disabled
        Continuous Transmitter..................: Disabled
        DECT-like Phone.........................: Disabled
        Video Camera............................: Disabled
        802.15.4................................: Disabled
        WiFi Inverted...........................: Enabled
        WiFi Invalid Channel....................: Enabled
        SuperAG.................................: Disabled
        Canopy..................................: Disabled
        Microsoft Device........................: Disabled
        WiMax Mobile............................: Disabled
        WiMax Fixed.............................: Disabled
    Interference Device Alarms..................: Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State.............: Disabled
    CleanAir Driven RRM Sensitivity.............: LOW
    CleanAir Persistent Devices state...........: Disabled
```

show ap dot11 cleanair summary

すべての 802.11a Cisco AP の CleanAir 設定を表示するには、**show ap dot11 cleanair summary** コマンドを使用します。

show ap dot11{**24ghz**| **5ghz**} **cleanair summary**

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
cleanair summary	すべての 802.11a Cisco AP の CleanAir 設定のサマリー

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

show ap dot11

802.11a および 802.11b の設定情報を表示するには、**showapdot11** コマンドを使用します。

show ap dot11{**24ghz**| **5ghz**} {**channel**| **coverage**| **group**| **load-info**| **logging**| **media-stream**| **monitor**| **network**| **profile**| **receiver**| **service-policy**| **summary**| **txpower**| **ccx global**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。

channel	自動チャネル割り当ての設定と統計情報を表示します。
coverage	カバレッジ ホール検出の設定と統計情報を表示します。
group	802.11a または 802.11b のシスコ無線 RF グループを表示します。
load-info	すべての Cisco AP のチャネルの使用率およびクライアント数の情報を表示します。
logging	802.11a または 802.11b の RF イベントとパフォーマンスのログを表示します。
media-stream	802.11a または 802.11b のメディア リソース予約制御の設定を表示します。
monitor	802.11a または 802.11b のデフォルトのシスコ無線モニタリングを表示します。
network	802.11a または 802.11b のネットワーク設定を表示します。
profile	802.11a または 802.11b の Lightweight アクセス ポイントのパフォーマンス プロファイルを表示します。
receiver	802.11a または 802.11b レシーバの設定と統計情報を表示します。
service-policy	すべてのシスコ アクセス ポイントの 802.11a または 802.11b 無線に関するサービス品質（QoS）ポリシーを表示します。
summary	802.11a または 802.11b の Cisco Lightweight アクセス ポイントの名前、チャネル、および送信レベルのサマリーを表示します。
txpower	802.11a または 802.11b の自動送信電力割り当てを表示します。
ccxglobal	デバイスに結合されたすべてのシスコ アクセス ポイントに関する 802.11a または 802.11b の Cisco Client eXtensions（CCX）情報を表示します。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**load-info** パラメータが追加されました。

次に、自動チャネル割り当ての設定および統計情報を表示する例を示します。

```
Device# show ap dot11 5ghz channel
Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 12 Hours
  Anchor time (Hour of the day)             : 20
  Channel Update Contribution               : SNI.
  Channel Assignment Leader                 : web (9.9.9.2)
  Last Run                                  : 13105 seconds ago
  DCA Sensitivity Level                     : MEDIUM (15 dB)
  DCA 802.11n Channel Width                 : 40 Mhz
  Channel Energy Levels
      Minimum                               : unknown
      Average                               : unknown
      Maximum                               : unknown
  Channel Dwell Times
      Minimum                               : unknown
      Average                               : unknown
      Maximum                               : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                      : 36,40,44,48,52,56,60,64,149,153,1
57,161
  Unused Channel List                       : 100,104,108,112,116,132,136,140,1
65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                      :
  Unused Channel List                       : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                     : Disabled
```

次に、カバレッジ ホール検出の統計情報を表示する例を示します。

```
Device# show ap dot11 5ghz coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
  802.11a Coverage Data Packet Percentage       : 50 %
  802.11a Coverage Data RSSI Threshold          : -80dBm
  802.11a Global coverage exception level       : 25
  802.11a Global client minimum exception level   : 3 clients
```

次に、シスコの無線 RF グループ設定を表示する例を示します。

```
Device# show ap dot11 5ghz group
Radio RF Grouping

  802.11a Group Mode                : STATIC
  802.11a Group Update Interval     : 600 seconds
  802.11a Group Leader              : web (10.10.10.1)
  802.11a Group Member              : web(10.10.10.1)
                                      nb1(172.13.21.45) (*Unreachable)
  802.11a Last Run                  : 438 seconds ago
```

```
  Mobility Agents RF membership information
  ------------------------------------------------------------
  No of 802.11a MA RF-members : 0
```

次に、802.11a RF イベント ログおよびパフォーマンス ログを表示する例を示します。

```
Device# show ap dot11 5ghz logging
RF Event and Performance Logging

  Channel Update Logging             : Off
  Coverage Profile Logging           : Off
  Foreign Profile Logging            : Off
  Load Profile Logging               : Off
  Noise Profile Logging              : Off
  Performance Profile Logging        : Off
  TxPower Update Logging             : Off
```

次に、802.11a メディア ストリームの設定を表示する例を示します。

```
Device# show ap dot11 5ghz media-stream
Multicast-direct                : Disabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio     : Auto
Max Allowed Streams Per Client    : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

次に、802.11b ネットワークの無線監視を表示する例を示します。

```
Device# show ap dot11 5ghz monitor
Default 802.11a AP monitoring

  802.11a Monitor Mode                          : Enabled
  802.11a Monitor Mode for Mesh AP Backhaul     : disabled
  802.11a Monitor Channels                      : Country channels
  802.11a RRM Neighbor Discover Type            : Transparent
  802.11a AP Coverage Interval                  : 180 seconds
  802.11a AP Load Interval                      : 60 seconds
  802.11a AP Noise Interval                     : 180 seconds
  802.11a AP Signal Strength Interval           : 60 seconds
```

次に、802.11a プロファイルのグローバル設定と統計情報を表示する例を示します。

```
Device# show ap dot11 5ghz profile
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
802.11a Global coverage exception level............ 80%
802.11a Global client minimum exception lev........ 3 clients
```

次に、802.11a プロファイルのネットワーク設定と統計情報を表示する例を示します。

```
Device# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
```

```
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
```

```
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

次に、802.11a プロファイルのグローバル設定と統計情報を表示する例を示します。

```
Device# show ap dot11 5ghz receiver
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
802.11a Global coverage exception level............ 80%
802.11a Global client minimum exception lev........ 3 clients
```

次に、802.11a プロファイルのグローバル設定と統計情報を表示する例を示します。

```
Device# show ap dot11 5ghz service-policy
```

次に、802.11b アクセス ポイント設定の要約を表示する例を示します。

```
Device# show ap dot11 5ghz summary
AP Name MAC Address       Admin State Operation State Channel TxPower
------- ----------------- ----------- --------------- ------- -------
CJ-1240 00:21:1b:ea:36:60 ENABLED     UP              161     1( )
CJ-1130 00:1f:ca:cf:b6:60 ENABLED     UP              56*     1(*)
```

次に、802.11a 伝送パワー コストの設定と統計情報を表示する例を示します。

```
Device# show ap dot11 5ghz txpower
Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Transmit Power Update Contribution      : SNI.
Transmit Power Assignment Leader        : web (10.10.10.1)
Last Run                                : 437 seconds ago
```

次に、802.11a 伝送パワー コストの設定と統計情報を表示する例を示します。

```
Device# show ap dot11 5ghz ccx global
 802.11a Client Beacon Measurements:
     disabled
```

show ap env summary

AP 環境のサマリーを表示するには、**show ap env summary** コマンドを使用します。

キーワードおよび引数はありません。

コマンド デフォルト

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、AP 環境のサマリーを表示する例を示します。

```
Device#show ap env summary
```

show ap ethernet statistics

すべての Cisco Lightweight アクセス ポイントに関するイーサネット統計情報を表示するには、**showapethernetstatistics** コマンドを使用します。

show ap ethernet statistics

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイントのイーサネット情報を表示する例を示します。

```
Device# show ap ethernet statistics
```

show ap gps-location summary

接続されているすべての Cisco AP の GPS 位置のサマリーを表示するには、**show ap gps-location summary** コマンドを使用します。

キーワードおよび引数はありません。

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
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、接続されているすべての Cisco AP の GPS 位置のサマリーを表示する例を示します。

```
Device# show ap gps-location summary
```

show ap groups

システム内に定義されているすべてのアクセスポイントグループに関する情報を表示するには、**showapgroups** コマンドを使用します。

show ap groups

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイント グループの情報を表示する例を示します。

```
Device# show ap groups
```

show ap groups extended

システム内に定義されているすべての AP グループの詳細情報を表示するには、**show ap groups extended** コマンドを使用します。

show ap groups extended

構文の説明

extended	システム内に定義されているすべてのAPグループの詳細情報を表示します。

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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

show ap image

Cisco Lightweight アクセス ポイントに存在しているイメージを表示するには、**showapimage** コマンドを使用します。

show ap image

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントに存在しているイメージを表示する例を示します。

```
Device# show ap image
```

show ap is-supported

AP モデルがサポートされているかどうかを確認するには、**show ap is-supported** コマンドを使用します。

show ap is-supported *model-part-number*

構文の説明

model-part-number	AP モデルの部品番号。例：AIR-LAP1142N-N-K9。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0E	このコマンドが導入されました。

次に、AP モデルがサポートされているかどうかを確認する例を示します。

```
Device# show ap is-supported AIR-LAP1142N-N-K9

AP Support: Yes
```

show ap join stats summary

特定のアクセス ポイントで最後に発生した結合エラーの詳細を表示するには、**show ap join stats summary** コマンドを使用します。

show ap join stats summary

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

802.11 無線インターフェイスの MAC アドレスを取得するには、アクセス ポイントで **show interface** コマンドを入力します。

次に、アクセス ポイントの結合情報を表示する例を示します。

```
Device# show ap join stats summary
Number of APs : 1

Base MAC        Ethernet MAC    AP Name               IP Address       Status

--------------- --------------- --------------------- ---------------- -------------
-
c8f9.f91a.aa80  0000.0000.0000  N A                   0.0.0.0          Not Joined
```

show ap link-encryption

リンク暗号化ステータスを表示するには、**show ap link-encryption** コマンドを使用します。

構文の説明

show ap link-encryption

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、リンク暗号化ステータスを表示する例を示します。

```
Device# show ap link-encryption
```

show ap mac-address

アクセス ポイントに関して収集された結合関連の統計情報、および最後の結合エラーの詳細を表示するには、**showapmac-address** コマンドを使用します。

show ap mac-address *mac-address* **join stats** {**detailed| summary**}

構文の説明

mac-address	アクセス ポイント Ethernet MAC アドレス、または 802.11 無線インターフェイスの MAC アドレス。
joinstats	シスコのアクセス ポイントの結合情報と統計情報を表示します。
detailed	収集されたすべての結合関連の統計情報を表示します。
summary	最後の結合エラーの詳細を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、デバイスを結合しようしている特定のアクセス ポイントの結合情報を表示する例を示します。

```
Device# show ap mac-address d0c2.8267.8b00 join stats detailed

Discovery phase statistics
  Discovery requests received                              : 6
  Successful discovery responses sent                      : 6
  Unsuccessful discovery request processing                : 0
  Reason for last unsuccessful discovery attempt           : Not applicable
  Time at last successful discovery attempt                : Nov 20 17:25:10.841
  Time at last unsuccessful discovery attempt              : Not applicable

Join phase statistics
  Join requests received                                   : 3
  Successful join responses sent                           : 3
  Unsuccessful join request processing                     : 0
  Reason for last unsuccessful join attempt                : Not applicable
  Time at last successful join attempt                     : Nov 20 17:25:20.998
  Time at last unsuccessful join attempt                   : Not applicable

Configuration phase statistics
  Configuration requests received                          : 8
  Successful configuration responses sent                  : 3
  Unsuccessful configuration request processing            : 0
  Reason for last unsuccessful configuration attempt       : Not applicable
  Time at last successful configuration attempt            : Nov 20 17:25:21.177
  Time at last unsuccessful configuration attempt          : Not applicable

Last AP message decryption failure details
  Reason for last message decryption failure               : Not applicable

Last AP disconnect details
  Reason for last AP connection failure                   : Number of message retransmission
 to the AP has reached maximum

Last join error summary
  Type of error that occurred last                         : AP got or has been disconnected

  Reason for error that occurred last                     : Number of message retransmission
 to the AP has reached maximum
  Time at which the last join error occurred               : Nov 20 17:22:36.438
```

次に、アクセス ポイントの結合情報を表示する例を示します。

```
Device# show ap mac-address d0c2.8267.8b00 join stats detailed

Is the AP currently connected to controller..... No
Time at which the AP joined this controller last time..... Aug 21 12:50:36:061
Type of error that occurred last..... Lwapp join request
rejected
Reason for error that occurred last..... RADIUS authorization
is pending for the AP
Time at which the last join error occurred..... Aug 21 12:50:34:374
```

show ap monitor-mode summary

チャネルに最適化されたモニタ モードの現在の設定を表示するには、**show ap monitor-mode summary** コマンドを使用します。

show ap monitor-mode summary

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、チャネルに最適化された監視モードの現在の設定を表示する例を示します。

```
Device# show ap monitor-mode summary

AP Name Ethernet MAC      Status   Scanning Channel List
------- -------------     -------- -------- ----------------
AP_004  xx:xx:xx:xx:xx:xx Tracking 1,6,11,  4
```

show ap name auto-rf

Cisco Lightweight アクセス ポイントの自動 RF 設定を表示するには、**show ap name auto-rf** コマンドを使用します。

show ap name *ap-name* **auto-rf dot11** {**24ghz**| **5ghz**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。

5ghz	5 GHz 帯域を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの自動 RF 情報を表示する例を示します。

```
Device# show ap name AP01 auto-rf dot11 24ghz

Number of Slots                                 : 2
AP Name                                         : TSIM_AP-1
MAC Address                                     : 0000.2000.02f0
Slot ID                                         : 0
Radio Type                                      : 802.11b/g
Subband Type                                    : All

Noise Information
  Noise Profile                                 : Failed
  Channel   1                                    :   24 dBm
  Channel   2                                    :   48 dBm
  Channel   3                                    :   72 dBm
  Channel   4                                    :   96 dBm
  Channel   5                                    :  120 dBm
  Channel   6                                    : -112 dBm
  Channel   7                                    :  -88 dBm
  Channel   8                                    :  -64 dBm
  Channel   9                                    :  -40 dBm
  Channel  10                                    :  -16 dBm
  Channel  11                                    :    8 dBm

Interference Information
  Interference Profile                          : Passed
  Channel   1                                    : -128 dBm @  0% busy
  Channel   2                                    :  -71 dBm @  1% busy
  Channel   3                                    :  -72 dBm @  1% busy
  Channel   4                                    :  -73 dBm @  2% busy
  Channel   5                                    :  -74 dBm @  3% busy
  Channel   6                                    :  -75 dBm @  4% busy
  Channel   7                                    :  -76 dBm @  5% busy
  Channel   8                                    :  -77 dBm @  5% busy
  Channel   9                                    :  -78 dBm @  6% busy
  Channel  10                                    :  -79 dBm @  7% busy
  Channel  11                                    :  -80 dBm @  8% busy

Rogue Histogram (20/40_ABOVE/40_BELOW)
    Channel  36                                  : 27/ 4/ 0
    Channel  40                                  : 13/ 0/ 0
    Channel  44                                  :  5/ 0/ 0
    Channel  48                                  :  6/ 0/ 1
```

```
    Channel  52                                      :  4/ 0/ 0
    Channel  56                                      :  5/ 0/ 0
    Channel  60                                      :  1/ 3/ 0
    Channel  64                                      :  3/ 0/ 0
    Channel 100                                      :  0/ 0/ 0
    Channel 104                                      :  0/ 0/ 0
    Channel 108                                      :  0/ 1/ 0

Load Information
  Load Profile                                     : Passed
  Receive Utilization                              : 10%
  Transmit Utilization                             : 20%
  Channel Utilization                              : 50%
  Attached Clients                                 : 0 clients

Coverage Information
  Coverage Profile                                 : Passed
  Failed Clients                                   : 0 clients

Client Signal Strengths
  RSSI -100 dBm                                    : 0 clients
  RSSI  -92 dBm                                    : 0 clients
  RSSI  -84 dBm                                    : 0 clients
  RSSI  -76 dBm                                    : 0 clients
  RSSI  -68 dBm                                    : 0 clients
  RSSI  -60 dBm                                    : 0 clients
  RSSI  -52 dBm                                    : 0 clients

Client Signal to Noise Ratios
  SNR    0 dB                                      : 0 clients
  SNR    5 dB                                      : 0 clients
  SNR   10 dB                                      : 0 clients
  SNR   15 dB                                      : 0 clients
  SNR   20 dB                                      : 0 clients
  SNR   25 dB                                      : 0 clients
  SNR   30 dB                                      : 0 clients
  SNR   35 dB                                      : 0 clients
  SNR   40 dB                                      : 0 clients
  SNR   45 dB                                      : 0 clients

Nearby APs
  AP 0000.2000.0300 slot 0                         : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0400 slot 0                         : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0600 slot 0                         : -68 dBm on  11 (10.10.10.1)

Radar Information

Channel Assignment Information
  Current Channel Average Energy                   : 0 dBm
  Previous Channel Average Energy                  : 0 dBm
  Channel Change Count                             : 0
  Last Channel Change Time                         : Wed Oct 17 08:13:36 2012
  Recommended Best Channel                         : 11

RF Parameter Recommendations
  Power Level                                      : 1
  RTS/CTS Threshold                                : 2347
  Fragmentation Threshold                          : 2346
  Antenna Pattern                                  : 0

Persistent Interference Devices
```

show ap name bhmode

Cisco ブリッジ バックホール モードを表示するには、**show ap name bhmode** コマンドを使用します。

構文の説明

show ap name *ap-name* **bhmode**

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの Cisco ブリッジ バックホール モードを表示する例を示します。

```
Device# show ap name TSIM_AP-1 bhmode
```

show ap name bhrate

Cisco ブリッジ バックホール レートを表示するには、**show ap name bhrate** コマンドを使用します。

show ap name *ap-name* **bhrate**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの Cisco ブリッジ バックホール レートを表示する例を示します。

```
Device# show ap name AP01 bhrate
```

show ap name cac voice

特定の Cisco Lightweight アクセス ポイントの音声コール アドミッション制御の詳細を表示するには、**show ap name cacvoice** コマンドを使用します。

show ap name *ap-name* **cac voice**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、特定のアクセス ポイントの音声コール アドミッション制御の詳細を表示する例を示します。

```
Device# show ap name AP01 cac voice
1) AP Name: AP01
==============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ------------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
```

```
3    1      1        maria-open            0           0
4    1      12       24                    0           0
```

show ap name config fnf

Cisco AP の NetFlow の入出力モニタを表示するには、**show ap name config fnf** コマンドを使用します。

show ap name *ap-name* **config fnf**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
fnf	Cisco AP の NetFlow の入出力モニタ。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

show ap name dot11 call-control

成功したコールのコール制御情報とメトリックを表示するには、**show ap name dot11 call-control** コマンドを使用します。

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **call-control** {**call-info**| **metrics**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。

call-info	コール情報を表示します。
metrics	コール メトリックを表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの成功したコールのメトリックを表示する例を示します。

```
Device# show ap name AP01 dot11 24ghz call-control metrics

Slot#   Call Count      Call Duration
---------------------------------
0       0               0
```

show ap name cable-modem

特定の AP の AP CAPWAP CCX を表示するには、**show ap name cable-modem** コマンドを使用します。

show ap name *ap-name***cable-modem**

構文の説明

ap-name	特定の AP の名前。

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
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、AP1 の AP CAPWAP CCX を表示する例を示します。

```
Device# show ap name ap1 cable-modem
```

show ap name capwap retransmit

Control And Provisioning of Wireless Access Points（CAPWAP）の再送信の設定を表示するには、**show ap name capwap retransmit** コマンドを使用します。

show ap name *ap-name* **capwap retransmit**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの CAPWAP の再送信の設定を表示する例を示します。

```
Device# show ap name AP01 capwap retransmit

AP Name   Retransmit Interval Retransmit Count
--------  ------------------- ----------------
AP01      3                   5
```

show ap name ccx rm

アクセス ポイントの Cisco Client Extension（CCX）無線管理ステータス情報を表示するには、**show ap name ccx rm** コマンドを使用します。

show ap name *ap-name* **ccx rm status**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの CCX 無線管理情報を表示する例を示します。

```
Device# show ap name AP01 ccx rm status

802.11b/g Radio
  Beacon Request                                : Disabled
  Channel Load Request                          : Disabled
  Frame Request                                 : Disabled
  Noise Histogram Request                       : Disabled
  Path Loss Request                             : Disabled
  Interval                                      : 60
  Iteration                                     : 0

802.11a Radio
  Beacon Request                                : Disabled
  Channel Load Request                          : Disabled
  Frame Request                                 : Disabled
  Noise Histogram Request                       : Disabled
  Path Loss Request                             : Disabled
  Interval                                      : 60
  Iteration                                     : 0
```

show ap name cdp

アクセス ポイントの Cisco Discovery Protocol（CDP）情報を表示するには、**show ap name cdp** コマンドを使用します。

show ap name *ap-name* **cdp** [**neighbors** [**detail**]]

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
neighbors	（任意）CDP を使用しているネイバーを表示します。
detail	（任意）CDP を使用している特定のアクセス ポイントのネイバーに関する詳細情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの CDP 情報を表示する例を示します。

```
Device# show ap name AP01 cdp neighbors detail
```

show ap name channel

特定のメッシュ アクセス ポイントの使用可能なチャネルを表示するには、**show ap name channel** コマンドを使用します。

show ap name *ap-name* **channel**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、特定のアクセス ポイントの使用可能なチャネルを表示する例を示します。

```
Device# show ap name AP01 channel

Slot ID                                          : 0
Allowed Channel List                             : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                   10, 11
Slot ID                                          : 1
Allowed Channel List                             : 36, 40, 44, 48, 52, 56, 60, 64, 100
                                                   104, 108, 112, 116, 132, 136, 140, 149,
 153
                                                   157, 161
```

show ap name config

特定の Cisco Lightweight アクセス ポイントの一般的な情報およびイーサネット VLAN タギング情報を表示するには、**show ap name config** コマンドを使用します。

show ap name *ap-name* **config** {**ethernet**| **general**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
ethernet	アクセス ポイントのイーサネット タギング設定情報を表示します。
general	アクセス ポイントの一般的な情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントのイーサネット タギング情報を表示する例を示します。

```
Device# show ap name AP01 config ethernet

VLAN Tagging Information for AP01
```

次に、アクセス ポイントの一般的な情報を表示する例を示します。

```
Device# show ap name AP01 config general

Cisco AP Name                                   : AP01
Cisco AP Identifier                             : 5
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : Unconfigured
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
Primary Cisco Controller Name                   : CAPWAP Controller
Primary Cisco Controller IP Address             : 10.10.10.1
Secondary Cisco Controller Name                 :
Secondary Cisco Controller IP Address           : Not Configured
Tertiary Cisco Controller Name                  :
Tertiary Cisco Controller IP Address            : Not Configured
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
```

```
Cisco AP System Logging Host                  : 255.255.255.255
AP Up Time                                    : 15 days 16 hours 19 minutes 57
 seconds
AP CAPWAP Up Time                             : 4 minutes 56 seconds
Join Date and Time                            : 10/18/2012 04:48:56
Join Taken Time                               : 15 days 16 hours 15 minutes 0
seconds
Join Priority                                 : 1
Ethernet Port Duplex                          : Auto
Ethernet Port Speed                           : Auto
AP Link Latency                               : Disabled
Rogue Detection                               : Disabled
AP TCP MSS Adjust                             : Disabled
AP TCP MSS Size                               : 6146
```

show ap name config dot11

特定の Cisco Lightweight アクセス ポイントに対応する 802.11 設定情報を表示するには、**show ap name config dot11** コマンドを使用します。

show ap name *ap-name* **config dot11** {**24ghz| 49ghz| 58ghz| 5ghz| dual-band**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
49ghz	802.11-4.9G ネットワークの設定を表示します。
58ghz	802.11-5.8G ネットワークの設定を表示します。
5ghz	5 GHz 帯域の設定を表示します。
dual-band	デュアル バンド無線の設定を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**dual-band** パラメータが追加されました。

次に、特定の Cisco Lightweight アクセス ポイントに対応する 802.11b 設定情報を表示する例を示します。

```
Device# show ap name AP01 config dot11 24ghz

Cisco AP Identifier                             : 5
Cisco AP Name                                   : AP01
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -A
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Mini IOS Version                                : 3.0.51.0
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 17 hours 9 minutes 41
seconds
AP CAPWAP Up Time                               : 54 minutes 40 seconds
Join Date and Time                              : 10/18/2012 04:48:56
Join Taken Time                                 : 15 days 16 hours 15 minutes 0
seconds

Attributes for Slot 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Administrative State                          : Enabled
  Operation State                               : Up
  Cell ID                                       : 0

  Station Configuration
    Configuration                               : Automatic
    Number of WLANs                             : 1
    Medium Occupancy Limit                      : 100
```

```
  CFP Period                                    : 4
  CFP Maximum Duration                          : 60
  BSSID                                         : 000020000200

  Operation Rate Set
     1000 Kbps                                  : MANDATORY
     2000 Kbps                                  : MANDATORY
     5500 Kbps                                  : MANDATORY
    11000 Kbps                                  : MANDATORY
     6000 Kbps                                  : SUPPORTED
     9000 Kbps                                  : SUPPORTED
    12000 Kbps                                  : SUPPORTED
    18000 Kbps                                  : SUPPORTED
    24000 Kbps                                  : SUPPORTED
    36000 Kbps                                  : SUPPORTED
    48000 Kbps                                  : SUPPORTED
    54000 Kbps                                  : SUPPORTED

  MCS Set
    MCS  0                                      : SUPPORTED
    MCS  1                                      : SUPPORTED
    MCS  2                                      : SUPPORTED
    MCS  3                                      : SUPPORTED
    MCS  4                                      : SUPPORTED
    MCS  5                                      : SUPPORTED
    MCS  6                                      : SUPPORTED
    MCS  7                                      : SUPPORTED
    MCS  8                                      : SUPPORTED
    MCS  9                                      : SUPPORTED
    MCS 10                                      : SUPPORTED
    MCS 11                                      : SUPPORTED
    MCS 12                                      : SUPPORTED
    MCS 13                                      : SUPPORTED
    MCS 14                                      : SUPPORTED
    MCS 15                                      : SUPPORTED
    MCS 16                                      : DISABLED
    MCS 17                                      : DISABLED
    MCS 18                                      : DISABLED
    MCS 19                                      : DISABLED
    MCS 20                                      : DISABLED
    MCS 21                                      : DISABLED
    MCS 22                                      : DISABLED
    MCS 23                                      : DISABLED

  Beacon Period                                 : 100
  Fragmentation Threshold                       : 2346
  Multi Domain Capability Implemented           : True
  Multi Domain Capability Enabled               : True
  Country String                                : US

Multi Domain Capability
  Configuration                                 : Automatic
  First Channel                                 : 0
  Number of Channels                            : 0
  Country String                                : US

MAC Operation Parameters
  Configuration                                 : Automatic
  Fragmentation Threshold                       : 2346
  Packet Retry Limit                            : 64
  Legacy Tx Beamforming Setting                 : Disabled

Tx Power
  Number of Supported Power Levels              : 8
  Tx Power Level 1                              : 20 dBm
  Tx Power Level 2                              : 17 dBm
  Tx Power Level 3                              : 14 dBm
  Tx Power Level 4                              : 11 dBm
  Tx Power Level 5                              : 8 dBm
  Tx Power Level 6                              : 5 dBm
  Tx Power Level 7                              : 2 dBm
  Tx Power Level 8                              : -1 dBm
  Tx Power Configuration                        : Automatic
```

```
    Current Tx Power Level                        : 1

  Phy OFDM Parameters
    Configuration                                 : Automatic
    Current Channel                               : 11
    Extension Channel                             : None
    Channel Width                                 : 20 MHz
    Allowed Channel List                          : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                    10, 11
    TI Threshold                                  : 0
    Antenna Type                                  : Internal
    Internal Antenna Gain (in .5 dBi units)       : 0
    Diversity                                     : Diversity enabled

    802.11n Antennas
      Tx                                          : A, B, C
      Rx                                          : A, B, C

  Performance Profile Parameters
    Configuration                                 : Automatic
    Interference Threshold                        : 10%
    Noise Threshold                               : -70 dBm
    RF Utilization Threshold                      : 80%
    Data Rate Threshold                           : 1000000 bps
    Client Threshold                              : 12 clients
    Coverage SNR Threshold                        : 15 dB
    Coverage Exception Level                      : 25%
    Client Minimum Exception Level                : 3 clients
    RTS/CTS Threshold                               : 2347
    Short Retry Limit                               : 7
    Long Retry Limit                                : 4
    Max Tx MSDU Lifetime                            : 512
    Max Rx Lifetime                                 : 512

  CleanAir Management Information
    CleanAir Capable                              : Yes
    CleanAir Management Admin State               : Enabled
    CleanAir Management Operation State           : Up
    Rapid Udpate Mode                             : Disabled
    Spectrum Expert connection                    : Disabled
    CleanAir NSI Key                              : 377313C8F290E246E640C4EF177BED
88
    Spectrum Expert connections counter           : 0
    CleanAir Sensor State                         : Configured

  Rogue Containment Information
    Containment Count                             : 0
```

show ap name config slot

特定のCisco Lightweightアクセス ポイント上のスロットの設定情報を表示するには、**show ap name config slot** コマンドを使用します。

show ap name *ap-name* **config slot** {**0**| **1**| **2**| **3**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
0	スロット番号 0 を表示します。
1	スロット番号 1 を表示します。

2	スロット番号 2 を表示します。
3	スロット番号 3 を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイント上のスロットの設定情報を表示する例を示します。

```
Device# show ap name AP01 config slot 0

Cisco AP Identifier                             : 3
Cisco AP Name                                   : AP01
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -A
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Mini IOS Version                                : 3.0.51.0
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
```

```
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 16 hours 1 minute 19 s
econds
AP CAPWAP Up Time                               : 20 hours 21 minutes 37 seconds

Join Date and Time                              : 10/17/2012 08:13:36
Join Taken Time                                 : 14 days 19 hours 39 minutes 41
 seconds

Attributes for Slot 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Administrative State                          : Enabled
  Operation State                               : Up
  Cell ID                                       : 0

  Station Configuration
    Configuration                               : Automatic
    Number of WLANs                             : 1
    Medium Occupancy Limit                      : 100
    CFP Period                                  : 4
    CFP Maximum Duration                        : 60
    BSSID                                       : 000020000200

    Operation Rate Set
       1000 Kbps                                : MANDATORY
       2000 Kbps                                : MANDATORY
       5500 Kbps                                : MANDATORY
      11000 Kbps                                : MANDATORY
       6000 Kbps                                : SUPPORTED
       9000 Kbps                                : SUPPORTED
      12000 Kbps                                : SUPPORTED
      18000 Kbps                                : SUPPORTED
      24000 Kbps                                : SUPPORTED
      36000 Kbps                                : SUPPORTED
      48000 Kbps                                : SUPPORTED
      54000 Kbps                                : SUPPORTED

    MCS Set
      MCS  0                                    : SUPPORTED
      MCS  1                                    : SUPPORTED
      MCS  2                                    : SUPPORTED
      MCS  3                                    : SUPPORTED
      MCS  4                                    : SUPPORTED
      MCS  5                                    : SUPPORTED
      MCS  6                                    : SUPPORTED
      MCS  7                                    : SUPPORTED
      MCS  8                                    : SUPPORTED
      MCS  9                                    : SUPPORTED
      MCS 10                                    : SUPPORTED
      MCS 11                                    : SUPPORTED
      MCS 12                                    : SUPPORTED
      MCS 13                                    : SUPPORTED
      MCS 14                                    : SUPPORTED
      MCS 15                                    : SUPPORTED
      MCS 16                                    : DISABLED
      MCS 17                                    : DISABLED
      MCS 18                                    : DISABLED
      MCS 19                                    : DISABLED
      MCS 20                                    : DISABLED
      MCS 21                                    : DISABLED
      MCS 22                                    : DISABLED
      MCS 23                                    : DISABLED
```

```
  Beacon Period                               : 100
  Fragmentation Threshold                     : 2346
  Multi Domain Capability Implemented         : True
  Multi Domain Capability Enabled             : True
  Country String                              : US

Multi Domain Capability
  Configuration                               : Automatic
  First Channel                               : 0
  Number of Channels                          : 0
  Country String                              : US

MAC Operation Parameters
  Configuration                               : Automatic
  Fragmentation Threshold                     : 2346
  Packet Retry Limit                          : 64

Tx Power
  Number of Supported Power Levels            : 8
  Tx Power Level 1                            : 20 dBm
  Tx Power Level 2                            : 17 dBm
  Tx Power Level 3                            : 14 dBm
  Tx Power Level 4                            : 11 dBm
  Tx Power Level 5                            : 8 dBm
  Tx Power Level 6                            : 5 dBm
  Tx Power Level 7                            : 2 dBm
  Tx Power Level 8                            : -1 dBm
  Tx Power Configuration                      : Automatic
  Current Tx Power Level                      : 1

Phy OFDM Parameters
  Configuration                               : Automatic
  Current Channel                             : 11
  Extension Channel                           : None
  Channel Width                               : 20 MHz
  Allowed Channel List                        : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                10, 11
  TI Threshold                                : 0
  Antenna Type                                : Internal
  Internal Antenna Gain (in .5 dBi units)     : 0
  Diversity                                   : Diversity enabled

  802.11n Antennas
    Tx                                        : A, B, C
    Rx                                        : A, B, C

Performance Profile Parameters
  Configuration                               : Automatic
  Interference Threshold                      : 10%
  Noise Threshold                             : -70 dBm
  RF Utilization Threshold                    : 80%
  Data Rate Threshold                         : 1000000 bps
  Client Threshold                            : 12 clients
  Coverage SNR Threshold                      : 15 dB
  Coverage Exception Level                    : 25%
  Client Minimum Exception Level              : 3 clients

Rogue Containment Information
  Containment Count                           : 0
```

show ap name core-dump

Lightweightアクセス ポイントのメモリ コア ダンプ情報を表示するには、**show ap name core-dump** コマンドを使用します。

構文の説明

show ap name *ap-name* **core-dump**

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、メモリ コア ダンプ情報を表示する例を示します。

```
Device# show ap name 3602a core-dump

TFTP server IP : 172.31.25.21
Memory core dump file : 3602a.dump
Memory core dump file compressed : Disabled
```

show ap name data-plane

特定の Cisco Lightweight アクセス ポイントのデータ プレーンのステータスを表示するには、**show ap name data-plane** コマンドを使用します。

show ap name *ap-name* **data-plane**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントのデータ プレーンのステータスを表示する例を示します。

```
Device# show ap name AP01 data-plane

                      Min Data         Data          Max Data     Last
AP Name              Round Trip     Round Trip     Round Trip    Update
------------------  --------------  --------------  -------------- --------
AP01                   0.000s          0.000s        0.000s       00:00:00
```

show ap name dot11

特定の Cisco Lightweight アクセス ポイントに対応する 802.11a または 802.11b 設定情報を表示するには、**show ap name dot11** コマンドを使用します。

show ap name *ap-name* **dot11** {**24ghz| 5ghz**} {**ccx| cdp| profile| service-policy output| stats| tsm** {**all**| *client-mac*}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
ccx	Cisco Client eXtensions（CCX）無線管理ステータス情報を表示します。
cdp	シスコ検出プロトコル（CDP）情報を表示します。
profile	802.11 プロファイルの設定と統計情報を表示します。
service-policyoutput	ダウンストリームのサービス ポリシー情報を表示します。
stats	Cisco Lightweight アクセス ポイントの統計情報を表示します。
tsm	802.11 トラフィック ストリーム メトリックの統計情報を表示します。
all	クライアントがアソシエーションを持つすべてのアクセス ポイントのリストを表示します。
client-mac	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、アクセスポイントに関連付けられたサービスポリシーを表示する方法を示します。

```
Device# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
Policy State : Installed
```

次の例では、特定のアクセス ポイントの CCX RRM 802.11 の設定を表示する例を示します。

```
Device# show ap name AP01 dot11 24ghz ccx
```

次の例では、特定のアクセス ポイントの CDP 情報を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz cdp

AP Name               AP CDP State
--------------------- --------------
AP03                  Disabled
```

次の例では、特定のアクセス ポイントの 802.11b プロファイルの設定と統計情報を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode            : GLOBAL
 802.11b Cisco AP Interference threshold              : 10 %
 802.11b Cisco AP noise threshold                     : -70 dBm
 802.11b Cisco AP RF utilization threshold            : 80 %
 802.11b Cisco AP throughput threshold                : 1000000 bps
 802.11b Cisco AP clients threshold                   : 12 clients
```

次の例では、特定のアクセスポイントのダウンストリームのサービスポリシー情報を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

次の例では、特定のアクセス ポイントの統計情報を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz stats
```

```
Number of Users................................: 0
TxFragmentCount................................: 0
MulticastTxFrameCnt............................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount.............................: 0
FrameDuplicateCount............................: 0
RtsSuccessCount................................: 0
RtsFailureCount................................: 0
AckFailureCount................................: 0
RxIncompleteFragment...........................: 0
MulticastRxFrameCnt............................: 0
FcsErrorCount..................................: 0
TxFrameCount...................................: 0
WepUndecryptableCount..........................: 0
TxFramesDropped................................: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).....: 0
  Video Bandwidth in use(% of config bw).....: 0
  Total BW in use for Voice(%)...............: 0
  Total BW in use for SIP Preferred call(%)..: 0

Load based Voice Call Stats
  Total channel MT free......................: 0
  Total voice MT free........................: 0
  Na Direct..................................: 0
  Na Roam....................................: 0

WMM TSPEC CAC Call Stats
  Total num of voice calls in progress.......: 0
  Num of roaming voice calls in progress.....: 0
  Total Num of voice calls since AP joined...: 0
  Total Num of roaming calls since AP joined.: 0
  Total Num of exp bw requests received......: 0
  Total Num of exp bw requests admitted......: 0
  Num of voice calls rejected since AP joined: 0
  Num of roam calls rejected since AP joined.: 0
  Num of calls rejected due to insufficent bw: 0
  Num of calls rejected due to invalid params: 0
  Num of calls rejected due to PHY rate......: 0
  Num of calls rejected due to QoS policy....: 0

SIP CAC Call Stats
  Total Num of calls in progress.............: 0
  Num of roaming calls in progress...........: 0
  Total Num of calls since AP joined.........: 0
  Total Num of roaming calls since AP joined.: 0
  Total Num of Preferred calls received......: 0
  Total Num of Preferred calls accepted......: 0
  Total Num of ongoing Preferred calls.......: 0
  Total Num of calls rejected(Insuff BW).....: 0
  Total Num of roam calls rejected(Insuff BW): 0

Band Select Stats
  Num of dual band client ...................: 0
  Num of dual band client added..............: 0
  Num of dual band client expired ...........: 0
  Num of dual band client replaced...........: 0
  Num of dual band client detected ..........: 0
  Num of suppressed client ..................: 0
  Num of suppressed client expired...........: 0
  Num of suppressed client replaced..........: 0
```

次の例では、特定のアクセスポイントに対応するすべてのクライアントのトラフィック ストリームの設定を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz tsm all
```

show ap name dot11 cleanair

アクセス ポイントに対応する CleanAir 設定情報を表示するには、**show ap name dot11 cleanair** コマンドを使用します。

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **cleanair** {**air-quality**| **device**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
cleanair	CleanAir 設定情報を表示します。
air-quality	CleanAir 電波品質（AQ）データを表示します。
device	5 GHz 帯域上にあるアクセス ポイントの CleanAir 干渉源を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、802.11b ネットワークのアクセス ポイントの CleanAir 電波品質情報を表示する例を示します。

```
Device# show ap name AP01 dot11 24ghz cleanair air-quality

AQ = Air Quality
DFS = Dynamic Frequency Selection
```

次に、802.11b ネットワークのアクセス ポイントの CleanAir 干渉源情報を表示する例を示します。

```
Device# show ap name AP01 dot11 24ghz cleanair device

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No ClusterID DevID Type AP Name ISI RSSI DC Channel
-- --------- ----- ---- ------- --- ---- ----------
```

show ap name env

特定の AP の AP 環境を表示するには、**show ap name env** コマンドを使用します。

show ap name *ap-name***env**

構文の説明

ap-name	特定の AP の名前。

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
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、AP1 の AP 環境を表示する例を示します。

```
Device# show ap name ap1 env
```

show ap name ethernet statistics

特定の Cisco Lightweight アクセス ポイントのイーサネット統計情報を表示するには、**show ap name ethernet statistics** コマンドを使用します。

show ap name *ap-name* **ethernet statistics**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントのイーサネット統計情報を表示する例を示します。

```
Device# show ap name 3602a ethernet statistics

Ethernet Stats for AP 3602a

Interface Name      Status   Speed       Rx Packets    Tx Packets    Discarded Packets

-------------------------------------------------------------------------------------
GigabitEthernet0    UP       1000 Mbps   3793          5036          0
```

show ap name eventlog

特定の Cisco Lightweight アクセス ポイントのイベント ログをダウンロードして表示するには、**show ap name eventlog** コマンドを使用します。

show ap name *ap-name* **eventlog**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、特定のアクセス ポイントのイベント ログを表示する例を示します。

```
Device# show ap name AP01 eventlog
```

show ap gps-location summary

接続されているすべての Cisco AP の GPS 位置のサマリーを表示するには、**show ap gps-location summary** コマンドを使用します。

キーワードおよび引数はありません。

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
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、接続されているすべての Cisco AP の GPS 位置のサマリーを表示する例を示します。

```
Device# show ap gps-location summary
```

show ap name image

指定されたアクセス ポイントの事前にダウンロードされたイメージに関する詳細情報を表示するには、**show ap name image** コマンドを使用します。

show ap name *ap-name* **image**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべてのアクセス ポイント上に存在しているイメージの表示の例を示します。

```
Device# show ap name 3602a image

Total number of APs  : 1

Number of APs
        Initiated                   : 0
        Predownloading              : 0
        Completed predownloading    : 0
        Not Supported               : 1
        Failed to Predownload       : 0

AP Name      Primary Image   Backup Image    Predownload Status    Predownload Ver...  Next
 Retry Time    Retry Count
-------------------------------------------------------------------------------------------------
3602a        10.0.1.234      0.0.0.0         Not supported         None                NA
                         0
```

show ap name inventory

アクセス ポイントのインベントリ情報を表示するには、**show ap name inventory** コマンドを使用します。

show ap name *ap-name* **inventory**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト
なし
コマンド モード
任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントのインベントリ情報を表示する例を示します。

```
Device# show ap name 3502b inventory

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 1140AG  ,  VID: V01,  SN: SIM1140K001


NAME:     , DESCR:
PID: ,  VID: ,  SN:


NAME:     , DESCR:
PID: ,  VID: ,  SN:
NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name lan port

LAN 情報を表示するには、**show ap name lan port** コマンドを使用します。

show ap name lan portsummary |*port-id*

構文の説明

summary	LAN 情報の概要を表示します。
port-id	LAN 情報が表示されるポートのポート ID。

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
Cisco IOS XE 3.7SE	このコマンドが導入されました。

次に、LAN 情報の概要を表示する例を示します。

```
Device# show ap name ap1 lan port summary
```

show ap name link-encryption

特定の Cisco Lightweight アクセス ポイントのリンク暗号化ステータスを表示するには、**show ap name link-encryption** コマンドを使用します。

show ap name *ap-name* **link-encryption**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、特定の Cisco Lightweight アクセス ポイントのリンク暗号化ステータスを表示する例を示します。

```
Device# show ap name AP01 link-encryption

                    Encryption  Dnstream  Upstream    Last
AP Name                  State     Count     Count  Update
------------------  ----------  --------  --------  ------
AP01                 Disabled         0         0   Never
```

show ap name service-policy

特定の Cisco Lightweight アクセス ポイントのサービス ポリシー情報を表示するには、**show ap name service-policy** コマンドを使用します。

show ap name *ap-name* **service-policy**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、特定の Cisco Lightweight アクセス ポイントのサービス ポリシー情報を表示する方法を示します。

```
Device# show ap name 3502b service-policy

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name tcp-adjust-mss

アクセス ポイントの TCP 最大セグメント サイズ（MSS）を表示するには、**show ap name tcp-adjust-mss** コマンドを使用します。

構文の説明

show ap name *ap-name* **tcp-adjust-mss**

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの TCP MSS を表示する例を示します。

```
Device# show ap name AP01 tcp-adjust-mss

AP Name                     TCP State        MSS Size
-------------------------------------------------------
AP01                        Disabled         6146
```

show ap name wlan

アクセス ポイントに定義された各 WLAN の基本サービス セット識別子（BSSID）値を表示し、WLAN の統計情報を表示するには、**show ap name wlan** コマンドを使用します。

show ap name *ap-name* **wlan** {**dot11** {**24ghz**| **5ghz**}| **statistic**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
dot11	802.11 パラメータを表示します。
24ghz	802.11b ネットワークの設定を表示します。
5ghz	802.11a ネットワークの設定を表示します。
statistic	WLAN の統計情報を表示します。

コマンド デフォルト

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、802.11b ネットワークのアクセス ポイントの BSSID 情報を表示する例を示します。

```
Device# show ap name AP01 wlan dot11 24ghz

Site Name                                       : default-group
Site Description                                :

WLAN ID  Interface  BSSID
-------------------------------------
1        default    00:00:20:00:02:00
12       default    00:00:20:00:02:0b
```

次に、アクセス ポイントの WLAN の統計情報を表示する例を示します。

```
Device# show ap name AP01 wlan statistic

WLAN ID  : 1
WLAN Profile Name  : maria-open

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0


WLAN ID  : 12
WLAN Profile Name  : 24

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0
```

show ap name wlandot11 service policy

アクセス ポイントの各基本サービス セット識別子（BSSID）の QoS ポリシーを表示するには、次のコマンドを使用します。

show apname*ap -name***wlandot1124ghzservice-policy**

show apname*ap -name***wlandot115ghzservice-policy**

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。

service-policy	アクセス ポイントのサービス ポリシー情報。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、各 BSSID の QoS ポリシーを表示する例を示します。

```
Deviceshow ap name <ap-name> wlan dot11 24ghz service-policy
```

show ap slots

接続されているすべての Cisco Lightweight アクセス ポイントのスロットの概要を表示するには、**show ap slots** コマンドを使用します。

show ap slots

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、接続されているすべての Cisco Lightweight アクセス ポイントのスロットの概要を表示する例を示します。

```
Controller# show ap slots

AP Name    Slots  AP Model    Slot0       Slot1      Slot2     Slot3
---------- ------ ----------- ----------- ---------- --------- --------
3602a      2      3502I       802.11b/g   802.11a    Unknown   Unknown
```

show ap summary

デバイスに接続されているすべての Cisco Lightweight アクセス ポイントのステータスの概要を表示するには、**show ap summary** コマンドを使用します。

show ap summary

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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して、各 Lightweight アクセス ポイント名、スロット数、製造者、MAC アドレス、ロケーション、デバイスのポート番号を含むリストを表示します。

次に、接続されているすべてのアクセス ポイントの要約を表示する例を示します。

```
Controller# show ap summary

Number of APs: 1

Global AP User Name: Cisco
Global AP Dot1x User Name: Not configured

AP Name                          AP Model  Ethernet MAC    Radio MAC       State
```

```
-------------------------------------------------------------------------------------
3602a                           3502I     003a.99eb.3fa8  d0c2.8267.8b00  Registered
```

show ap tcp-adjust-mss

Cisco Lightweight アクセス ポイントの TCP 最大セグメント サイズ（MSS）に関する情報を表示するには、**show ap tcp-adjust-mss** コマンドを使用します。

show ap tcp-adjust-mss

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクセス ポイントの TCP MSS 情報に関する情報を表示する例を示します。

```
Controller# show ap tcp-adjust-mss

AP Name                     TCP State        MSS Size
-------------------------------------------------------
3602a                       Disabled         0
```

show ap universal summary

接続されているすべての Cisco AP の一般的な概要を表示するには、**show ap universal summary** コマンドを使用します。

キーワードおよび引数はありません。

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
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、接続されているすべての Cisco AP の一般的な概要を表示する例を示します。

```
Device# show ap universal summary
```

show ap uptime

接続されているすべての Cisco Lightweight アクセス ポイントの稼働時間を表示するには、**show ap uptime** コマンドを使用します。

show ap uptime

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、接続されているすべてのアクセス ポイントの稼働時間を表示する例を示します。

```
Controller# show ap uptime

Number of APs : 1

Global AP User Name : Cisco
Global AP Dot1x User Name : Not configured

AP Name Ethernet MAC    AP Up Time                    Association Up Time

------- --------------- ------------------------------ ------------------------------
```

```
3602a   003a.99eb.3fa8  5 hours 13 minutes 40 seconds  5 hours 12 minutes 15 seconds
```

show wireless ap summary

すべてのワイヤレス アクセス ポイントのステータスの概要を表示するには、**show wireless ap summary** コマンドを使用します。

show wirelessap summary

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
10.4	このコマンドが追加されました。

次に、すべてのワイヤレス アクセス ポイントの概要を表示する例を示します。

```
Controller# show wireless ap summary
Sub-Domain Access Point Summary

Maximum AP limit: 1010
Total AP Licence Installed: 1000
Total AP Licence Available: 1000
Total AP joined :0
```

show wireless client ap

Cisco Lightweight アクセス ポイント上のクライアントを表示するには、**show wireless client ap** コマンドを使用します。

構文の説明

~~**show wireless client ap [name** *ap-name*~~] ~~**dot11 {24ghz| 5ghz}**~~	
name *ap-name*	（任意）Cisco Lightweight アクセス ポイントの名前を表示します。

dot11	802.11 パラメータを表示します。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 client ap コマンドでは自動的に無効にされたクライアントのステータスが表示されることがあります。除外リスト（ブラック リスト）のクライアントを表示するには、**show exclusionlist** コマンドを使用します。

次に、2.4 GHz 帯域の特定の Cisco Lghtweight アクセス ポイントのクライアント情報を表示する例を示します。

```
Device# show wireless client ap name AP01 dot11 24ghz

MAC Address       AP Id  Status     WLAN Id Authenticated
----------------- ------ ---------- ------- -------------
xx:xx:xx:xx:xx:xx 1      Associated 1       No
```

test ap name

アクセス ポイントとデバイス間のパスの最大伝送ユニット（MTU）の自動テストを有効にするには、**test ap name** コマンドを使用します。

test ap name *ap-name* **pmtu** {**disable size** *size*| **enable**}

構文の説明

ap-name	ターゲットの Cisco Lightweight アクセス ポイントの名前。

pmtu	アクセス ポイントの MTU 設定をテストします。
disable	パス MTU のテストを無効にし、MTU 値（バイト単位）を手動で設定します。
size*size*	パス MTU のサイズを指定します。 （注） 範囲は 576 ～ 1700 です。
enable	アクセス ポイントのパス MTU のテストを有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、デバイスに関連付けられているすべてのアクセス ポイントのパス MTU 設定を無効にする例を示します。

```
Controller# test ap name 3602a pmtu enable
```

test capwap ap name

特定の Cisco Lightweight アクセス ポイントの Control And Provisioning of Wireless Access Points（CAPWAP）パラメータをテストするには、**test capwap ap name** コマンドを使用します。

test capwap ap name *ap-name* {**encryption** {**enable| disable**}| **message** *token*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
encryption	Datagram Transport Layer Security（DTLS）暗号化をテストします。

enable	DTLS 暗号化が有効になっているかどうかをテストします。
disable	DTLS 暗号化が無効になっているかどうかをテストします。
message *token*	送信する RRM ネイバー メッセージを指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、特定のアクセス ポイントで DTLS 暗号化が有効になっているかどうかをテストする例を示します。

```
Controller# test capwap ap name 3602a encryption enable
```

次に、特定のアクセス ポイントで DTLS 暗号化が無効になっているかどうかをテストする例を示します。

```
Controller# test capwap ap name 3602a encryption disable
```

trapflags ap

特定の Cisco lightweight アクセス ポイント トラップの送信を有効にするには、**trapflags ap** コマンドを使用します。特定の Cisco lightweight アクセス ポイント トラップの送信を無効にするには、このコマンドの **no** 形式を使用します。

trapflags ap {**register**| **interfaceup**}

no trapflags ap {**register**| **interfaceup**}

構文の説明

register	Cisco Lightweight アクセス ポイントを Cisco スイッチに登録する場合、トラップの送信を有効にします。

interfaceup	Cisco Lightweight アクセス ポイント インターフェイス（A または B）が表示された場合に、トラップの送信をイネーブルにします。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、トラップで、アクセス ポイント関連トラップの送信が行われないようにする例を示します。

```
Device(config)# no trapflags ap register
```

wireless wps rogue ap rldp alarm-only

不正が検出された場合のアラームを設定するには、**wirelesswps rogueaprldp alarm-only** コマンドを使用します。アラームを無効にするには、このコマンドの **no** 形式を使用します。

[no]wireless wps rogue ap rldp alarm-onlymonitor-ap-only

構文の説明

monitor-ap-only	モニタ AP のみで RLDP を実行します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.7.3E	コマンドの **no** 形式が導入されました。

例

次に、検出された不正に対するアラームを設定する例を示します。

```
Device(config)wireless wps rogue ap rldp alarm-only
```

wireless wps rogue ap rldp auto-contain

不正が検出された場合の RLDP、アラーム、自動阻止を設定するには **wirelesswps rogueaprldp auto-contain** コマンドを使用します。アラームを無効にするには、このコマンドの no 形式を使用します。

[no]wireless wps rogue ap rldp auto-containmonitor-ap-only

構文の説明

monitor-ap-only	モニタ AP のみで RLDP を実行します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.7.3E	コマンドの **no** 形式が導入されました。

例

次に、検出された不正に対するアラームを設定する例を示します。

```
Devicewireless wps rogue ap rldp auto-contain
```

第 X 部

Mobility

- MPLS コマンド，699 ページ

第 11 章

MPLS コマンド

- mobility anchor, 699 ページ
- wireless mobility, 701 ページ
- wireless mobility controller, 701 ページ
- wireless mobility controller (ip_address) , 703 ページ
- wireless mobility controller peer-group, 704 ページ
- wireless mobility group keepalive, 705 ページ
- wireless mobility group member ip, 706 ページ
- wireless mobility group name , 707 ページ
- wireless mobility load-balance, 708 ページ
- show wireless mobility, 709 ページ
- clear wireless mobility statistics, 710 ページ

mobility anchor

モビリティ スティッキ アンカリングを設定するには、**mobility anchor sticky** コマンドを使用します。スティッキ アンカリングを無効にするには、このコマンドの **no** 形式を使用します。

ゲスト アンカリングを設定するには、**mobility anchor***ip-address* コマンドを使用します。

ゲスト アンカーを削除するには、このコマンドの **no** 形式を使用します。

デバイスを自動アンカーとして設定するには、**mobility anchor** コマンドを使用します。

mobility anchor {*ip-address*| **sticky**}

no mobility anchor {*ip-address*| **sticky**}

構文の説明

sticky	クライアントは、関連付けられている最初のスイッチにアンカーされます。 （注） このコマンドはデフォルトで有効になっており、低ローミング遅延を保証します。これは、クライアントがモビリティ ドメインに参加し、ドメイン内をローミングする場合でも、クライアントの Point of Presence のが変更されないように確保します。
ip-address	ゲスト アンカー デバイスの IP アドレスをこの WLAN に設定します。

コマンド デフォルト

スティッキ設定は、デフォルトでは有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE リリースより前の自動アンカー設定ではデバイス IP アドレスを入力する必要がありました。このリリースでは、IP アドレスが指定されていない場合、デバイス自身がアンカーになります。明示的に IP アドレスを指定する必要はありません。

使用上のガイドライン

- wlan_id または guest_lan_id は必ず指定し、無効にする必要があります。
- 1 つ目のモビリティ アンカーを設定するときに、WLAN または有線ゲスト LAN で自動アンカー モビリティを有効にします。
- 最後のアンカーを削除すると、自動アンカー モビリティ機能は無効になり、新しいアソシエーションに対しては標準のモビリティが再度使用されるようになります。
- モビリティは、ファイアウォールの通過が許可されている次のポートを使用します。
  - 16666
  - 16667
  - 16668

次に、スティッキ モビリティ アンカーを有効にする例を示します。
```
Device(config-wlan)# mobility anchor sticky
```

次に、ゲスト アンカリングを設定する例を示します。
```
Device(config-wlan)# mobility anchor 209.165.200.224
```

次に、デバイスを自動アンカーとして設定する例を示します。
```
Device(config-wlan)# mobility anchor
```

wireless mobility

間のモビリティ マネージャを設定するには、**wireless mobility** コマンドを使用します。

wireless mobility {**dscp** *value*}

構文の説明

dscp*value*	モビリティの 間の DSCP 値を設定します。

コマンド デフォルト

デフォルトの DSCP 値は、48 です。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、 間の DSCP 値が 20 のモビリティを設定する例を示します。
```
Device(config)# wireless mobility dscp 20
```

wireless mobility controller

モビリティ コントローラの設定を構成するには、**wireless mobility controller** コマンドを使用します。モビリティ コントローラの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。

wireless mobility controller peer-group *peer-group-name* [**bidge-domain-id** *id*| **member ip** *ip-address* [**public-ip**| *public-ip-address*]| **multicast ip** *multicast-address*]

no **wireless mobility controller peer-group** *peer-group-name* [**bidge-domain-id** *id*| **member ip** *ip-address* [**public-ip**| *public-ip-address*]| **multicast ip** *multicast-address*]

構文の説明

peer-group*peer-group-name*	モビリティ ピア グループを作成します。
bidge-domain-id*id*	モビリティ ピア グループのブリッジ ドメイン ID を設定します。
memberip*ip-address***public-ip***public-ip-address*	ピア グループ メンバーを追加または削除します。 （注） **public-ip***public-ip-address* はオプションで、モビリティ ピアが NAT 処理されている場合にのみ使用します。
multicastip*multicast-address*	ピア グループのマルチキャスト設定を構成します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

コンバージド アクセス ソリューションでは、WLAN は VLAN にマッピングされ、VLAN は通常サブネットにマッピングされます。シームレスなローミングのため、2 つのコントローラに設定されている同じ VLAN は、同じサブネットにマッピングされることが期待されます。ローミング イベントを処理するコントローラは、次の処理が必要かどうかを判断しなければならないため、1 つのコントローラから次のコントローラへのマッピングが一致していることは、ローミングの際に重要です。

- レイヤ 2 ローミング イベントの解決（WLAN から VLAN およびサブネットへのマッピングがアンカーと外部コントローラで一致している場合）、または
- レイヤ 3 ローミング イベントの解決（WLAN から VLAN およびサブネットへのマッピングがアンカーと外部コントローラで異なっている場合）。

この判断は、コントローラ間での WLAN SSID の文字列と VLAN ID の比較によって実行されます。WLAN SSID と VLAN ID が一致する場合、VLAN に関連付けられたサブネットも一致することが予想されます。

このマッピングが一致しない場合もあります。たとえば、コントローラ 1 の WLAN1 が VLAN 14 にマッピングされ、コントローラ 1 の VLAN 14 がサブネット 10.10.14.0/24 にマッピングされているとします。同時に、コントローラ 2 の WLAN 1 は VLAN 14 にマッピングされているものの、コントローラ 2 の VLAN 14 がサブネット 172.31.24.0/24 にマッピングされているとします。コントローラ 1 と 2 は、WLAN 1 と関連付けられた VLAN を比較してレイヤ 2 ローミング イベントを処理していると判断しますが、実際には、VLAN 14 が両コントローラに対して持つレイヤ 3 としての意味が異なるため、このローミング イベントはレイヤ 3 です。

VLAN と関連付けられたサブネットとの接続が解除された場合、さまざまなブリッジ ドメイン ID に対してコンバージド アクセス コントローラを設定することもできます。同じブリッジ ドメイン ID の 2 つのコントローラは、同じ VLAN でサブネット マッピングされると想定されます。サブネット マッピング用に同じ VLAN を共有し、ローミングが予想されるすべてのコントローラに、同じブリッジ ドメイン ID を設定することをお勧めします。

次に、 ブリッジ ドメイン ID を設定する例を示します。

```
Device (config)# wireless mobility controller peer-group SPG1 bridge-domain-id 111
```

次に、ブリッジ ID が 111 の ピア グループを作成し設定する例を示します。

```
Device(config)# controller peer-group TestDocPeerGroup bridge-domain-id 111
```

次に、ブリッジ ID が 111 の ピア グループを無効にする例を示します。

```
Device(config)# no controller peer-group TestDocPeerGroup bridge-domain-id 111
```

次に、NAT 処理されたメンバーを設定する例を示します（IP 172.19.13.15 は NAT の範囲 外）。

```
Device (config)# wireless mobility group ip 1.4.91.2 public-ip 172.19.13.15
```

次に、NAT 処理されないメンバーを設定する例を示します（IP 1.4.91.2 は NAT の範囲内）。

```
Device (config)# wireless mobility group ip 1.4.91.2
```

wireless mobility controller (ip_address)

モビリティ コントローラを設定するには、**wirelessmobilitycontroller** コマンドを使用します。

MC から MA にスイッチを変換するには、このコマンドの **no wirelessmobilitycontroller** 形式を使用します。

モビリティ コントローラの IP アドレスを削除するには、**nowirelessmobilitycontroller**ip-address を使用します。

wireless mobility controller [**ip** *ip-address* [**public-ip** *public-ip-address*]]

no wireless mobility controller

no wireless mobility controllerip*ip-address*

構文の説明

ip*ip-address*	モビリティ コントローラの IP アドレス。
public-ip*public-ip-address*	

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
Cisco IOS XE 3.2SE	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、コンバージド アクセス スイッチに対してのみ有効です。

NAtedアドレスは通信の確立に使用され、設定済みのワイヤレス管理インターフェイスは、CAPWAP交換時にピア コントローラを特定するために使用されます。

次に、コントローラがワイヤレス管理インターフェイスと通信する例を示します。

```
Device (config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6
```

次に、ターゲット コントローラが NAT を使用する場合に、ワイヤレス管理インターフェイスとともに NAT オプションを追加する例を示します。

```
Device (config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.21.21.2
```

wireless mobility controller peer-group

モビリティ ピア グループを設定するには **wireless mobility controller peer-group** コマンドを使用し、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。

wireless mobility controller peer-group *peer-group* **member IP** *ip-address***mode centralized**

構文の説明

peer group	ピア グループの名前。
member IP	ピア グループ メンバーを追加します。
ip-address	追加するピア グループ メンバーの IP アドレス。
mode centralized	集約的に管理されるピア グループ メンバーの管理モードを設定します。

コマンド デフォルト

集約型モードはオフです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

```
Device enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mobility controller peer-group peer1 member ip 10.0.0.1 mode
centralized
```

wireless mobility group keepalive

モビリティ グループ パラメータを設定し、その ping パラメータをキープアライブにするには、**wireless mobility group keepalive** コマンドを使用します。モビリティ グループ 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。

wireless mobility group keepalive {**count** *number*| **interval** *interval*}

no wireless mobility group keepalive {**count** *number*| **interval** *interval*}

構文の説明

count*number*	モビリティ グループ メンバに ping 要求を送信する回数。この回数を超えると、メンバにはアクセスできないと見なされます。有効な範囲は3～20です。デフォルトは 3 です。
interval*interval*	モビリティ グループ メンバへの ping 要求の送信間隔。範囲は 1 ～ 30 秒です。デフォルト値は 10 秒です。

コマンド デフォルト

カウントは 3秒、間隔は 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

interval のデフォルト値は 10 秒、*retries* のデフォルト値は 3 秒に設定されます。

次に、モビリティ グループ メンバに送信する各 ping 要求の間隔を 10 秒に指定する例を示します。

```
Device(config)# wireless mobility group keepalive count 10
```

wireless mobility group member ip

モビリティ グループ メンバー リストでユーザの追加または削除を行うには、**wireless mobility group member ip** コマンドを使用します。モビリティ グループからメンバーを削除するには、このコマンドの **no** 形式を使用します。

wireless mobility group member ip *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*]

no wireless mobility group member ip *ip-address*

構文の説明

ip-address	メンバー コントローラの IP アドレス。
public-ip*public-ip-address*	（任意）メンバー コントローラのパブリック IP アドレス。 （注） このコマンドは、メンバーが NAT に関与する場合にのみ使用されます。サポートされているのは、スタティック IP NAT のみです。
group*group-name*	（任意）メンバー コントローラのグループ名。 （注） このコマンドは、メンバーがローカル モビリティ コントローラと同じグループに追加されない場合にのみ使用されます。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

モビリティ グループは、特定の導入に複数のモビリティ コントローラ（MC）がある場合に使用されます。モビリティグループに任意の名前を割り当てることもできますし、デフォルトグループの名前を割り当てることもできます。モビリティグループメンバーは、グループ内でローミングするグループのすべてのメンバーに対して設定する必要があります。

次に、モビリティ グループにメンバーを追加する例を示します。

```
Device(config)# mobility group member ip 10.104.171.101 group TestDocGroup
```

wireless mobility group name

モビリティ ドメイン名を設定するには、**wirelessmobilitygroupname** コマンドを使用します。モビリティ ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

（注） ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

wireless mobility group name *domain-name*

no wireless mobility group name

構文の説明

domain-name	次のコマンドを入力して、新しいモビリティ グループを作成します。ドメイン名は最大 31 文字で、大文字と小文字を区別します。

コマンド デフォルト

これがデフォルトです。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、モビリティ ドメイン名 lab1 を設定する例を示します。

```
Device(config)# mobility group domain lab1
```

wireless mobility load-balance

このコマンドは、少なくともロードされ、モバイル クライアントの Point of Presence として機能するよう選択されたスイッチ ピア グループ（SPG）のモビリティ アンカー（MA）でモバイル クライアントをロード バランシングするために使用されます。

モビリティ ロード バランスのステータスを設定するには、**wirelessmobilityload-balance** コマンドを使用します。

モビリティ ロード バランスを無効にするには、このコマンドの **nowirelessmobilityload-balance** 形式を使用します。

モビリティ ロードバランスがオンになっているスイッチでクライアント ロードを設定するには、このコマンドの **nowirelessmobilityload-balance**threshold 形式を使用します。

wireless mobility load-balance [**threshold** *threshold*]

[**no**]**wireless mobility load-balance [threshold]**

[**no**]**wireless mobility load-balance**

構文の説明

threshold*threshold*	ローカルで固定できるクライアント数のしきい値を設定します。

コマンド デフォルト

ロード バランスは有効で、値は 1000 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
Cisco IOS XE 3.2SE	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、モビリティ エージェントのみでサポートされます。
- デフォルトでは、しきい値はノードの総クライアント数の 50 パーセント以上を入力できます。設定されたしきい値に達した後にスイッチに追加されたクライアントは、同じスイッチピア グループ内の最小限のロード済みスイッチに自動的に固定されます。

次に、しきい値を 150 に設定したモビリティ ロード バランス ステータスを設定する例を示します。

```
Device(config)# wireless mobility load-balance threshold 150
```

show wireless mobility

ワイヤレス モビリティの概要を表示するには、**show wireless mobility** コマンドを使用します。

showwirelessmobility{**load-balance summary agent***mobility-agent-ip***client summary**|**ap-listip-address***ip-address*|**controller client summary**|**dtls connections**|**statistics summary**}

構文の説明

load-balance summary	モビリティのロード バランスのプロパティを表示します。
agent *mobility-agent-ip* **client summary**	モビリティ エージェントのアクティブ クライアントを表示します。
ap-list ip-address *ip-address*	モビリティ グループに認識されている Cisco AP のリストを表示します。
controller client summary	サブドメインのアクティブ クライアントを表示します。
dtls connections	DTLS サーバのステータスを表示します。
statistics	Mobility Manager の統計を表示します。
summary	Mobility Manager のサマリーを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、Mobility Manager のサマリーを表示する例を示します。

```
Device (config)# show wireless mobility ap-list

AP name                          AP radio MAC      Controller IP     Learnt from
-------------------------------------------------------------------------------------------------
TSIM_AP-101                      0000.2000.6600    9.9.9.2           Self
TSIM_AP-102                      0000.2000.6700    9.9.9.2           Self
TSIM_AP-103                      0000.2000.6800    9.9.9.2           Self
TSIM_AP-400                      0000.2001.9100    9.9.9.2           Self
TSIM_AP-402                      0000.2001.9300    9.9.9.2           Self
TSIM_AP-403                      0000.2001.9400    9.9.9.2           Self
TSIM_AP-406                      0000.2001.9700    9.9.9.2           Self
TSIM_AP-407                      0000.2001.9800    9.9.9.2           Self
TSIM_AP-409                      0000.2001.9a00    9.9.9.2           Self
```

clear wireless mobility statistics

ワイヤレス統計情報をクリアするには、**clear wireless mobility statistics** コマンドを使用します。

clear wireless mobility statistics

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

clearwirelessmobilitystatistics コマンドを使用すると、すべての情報をクリアできます。

次に、ワイヤレス モビリティ統計情報をクリアする例を示します。

```
Device (config)# clear wireless mobility statistics
```

第 XI 部

マルチプロトコル ラベル スイッチング（MPLS）

- MPLS コマンド，715 ページ

第 12 章

MPLS コマンド

- mpls ip default-route, 715 ページ
- mpls ip（グローバル コンフィギュレーション）, 716 ページ
- mpls ip（インターフェイス コンフィギュレーション）, 718 ページ
- mpls label protocol（グローバル コンフィギュレーション）, 719 ページ
- mpls label protocol（インターフェイス コンフィギュレーション）, 720 ページ
- mpls label range, 721 ページ
- show mpls label range, 723 ページ

mpls ip default-route

IPデフォルトルートに関連付けられたラベルの配信を有効にするには、グローバル コンフィギュレーション モードで **mpls ip default-route** コマンドを使用します。

mpls ip default-route

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IP デフォルト ルートのラベルの配信はありません。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

mpls ip default-route コマンドを使用する前に、ダイナミック ラベル スイッチング（つまり、ルーティング プロトコルに基づくラベルの配信）を有効にする必要があります。

次に、IP デフォルト ルートに関連付けられたラベルの配信を有効にする例を示します。

```
Switch# configure terminal
Switch(config)# mpls ip
Switch(config)# mpls ip default-route
```

関連コマンド

コマンド	説明
mpls ip（グローバル コンフィギュレーション）	プラットフォーム用に通常ルーティングされるパスに沿って IPv4 パケットの MPLS 転送が行われるようにします。
mpls ip（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用に通常ルーティングされるパスに沿って IPv4 パケットの MPLS 転送が行われるようにします。

mpls ip（グローバル コンフィギュレーション）

プラットフォームの通常のルーテッド パスでの IPv4 および IPv6 パケットのマルチプロトコル ラベル スイッチング（MPLS）転送を有効にするには、グローバル コンフィギュレーション モードで **mpls ip** 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。

mpls ip

no mpls ip

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

プラットフォームの通常のルーテッド パスでの IPv4 および IPv6 パケットのラベル スイッチングは有効になっています。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

通常のルーテッド パスでの IPv4 および IPv6 パケットの MPLS 転送（ダイナミック ラベル スイッチングと呼ばれることもある）は、このコマンドによって有効になります。ダイナミック ラベル スイッチングを実行するように指定されたインターフェイスには、そのインターフェイス用およびプラットフォーム用にこのスイッチング機能がイネーブルになっていなければなりません。

このコマンドの **no** 形式は、インターフェイスの設定に関係なく、すべてのプラットフォーム インターフェイスのダイナミック ラベル スイッチングを停止します。また、ダイナミック ラベル スイッチングのためのラベルの配信も停止します。ただし、このコマンドの no 形式は、ラベル スイッチ パス（LSP）トンネルを介してのラベルの付いたパケットの送信には影響しません。

次に、プラットフォームのダイナミック ラベル スイッチングをディセーブルにし、プラットフォームのすべてのラベル配信を停止させる例を示します。

```
Switch(config)# no mpls ip
```

関連コマンド

コマンド	説明
mpls ip（インターフェイス コンフィギュレーション）	関連付けられているインターフェイスの通常のルーテッド パスでの IPv4 および IPv6 パケットの MPLS 転送を有効にします。

mpls ip（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の通常のルーテッド パスでの IPv4 パケットおよび IPv6 パケットのマルチプロトコル ラベル スイッチング（MPLS）フォワーディングを有効にするには、インターフェイス コンフィギュレーション モードで **mpls ip** コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。

mpls ip

no mpls ip

構文の説明

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

インターフェイスの通常のルーテッドパスでIPv4パケットおよびIPv6パケットをMPLSフォワーディングする機能は無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

通常のルーテッド パスで IPv4 パケットおよび IPv6 パケットを MPLS フォワーディングする機能は、ダイナミック ラベル スイッチングとも呼ばれます。プラットフォームでダイナミック ラベル スイッチングがイネーブルになっている場合、インターフェイス上でこのコマンドを実行すると、ネイバー探索 HELLO メッセージの定期送信によりインターフェイスでラベル配布が開始されます。インターフェイスを経由してルーティングされる宛先の出ラベルがわかっている場合、宛先のパケットにその出ラベルが付され、インターフェイスを経由してフォワーディングされます。

このコマンドの **no** 形式を使用すると、インターフェイスを経由してルーティングされるパケットはラベルなしで送信されます。また、インターフェイスのラベル配布も終了します。しかし、このインターフェイスを使用するリンクステート パケット（LSP）トンネルを経由するラベル付きパケットの送信が、コマンドの no 形式による影響を受けることはありません。

次に、イーサネット インターフェイスでラベル スイッチングを有効にする例を示します。

```
Switch(config)# configure terminal
Switch(config-if)# interface TenGigabitEthernet1/0/3
Switch(config-if)# mpls ip
```

次に、Cisco Catalyst スイッチの指定された VLAN インターフェイス（SVI）でラベル スイッチングを有効にする例を示します。

```
Switch(config)# configure terminal
Switch(config-if)# interface vlan 1
Switch(config-if)# mpls ip
```

mpls label protocol（グローバル コンフィギュレーション）

プラットフォームの Label Distribution Protocol（LDP; ラベル配布プロトコル）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 **mpls label protocol** コマンドを使用します。デフォルト LDP に戻すには、このコマンドの **no** 形式を使用します。

mpls label protocol ldp

no mpls label protocol ldp

構文の説明

LDP	LDP をデフォルトのラベル配布プロトコルとすることを指定します。

コマンド デフォルト

LDP がデフォルトのラベル配布プロトコルです。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

global mpls label protocol ldp コマンドまたは interface mpls label protocol ldp コマンドのどちらも使用されていない場合は、すべてのラベル配布セッションで LDP が使用されます。

次のコマンドは、LDP をプラットフォームのラベル配布プロトコルとして確立します。

```
Switch(config)# mpls label protocol ldp
```

mpls label protocol（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 Label Distribution Protocol（LDP; ラベル配布プロトコル）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 **mpls label protocol** コマンドを使用します。インターフェイスから LDP を削除するには、このコマンドの **no** 形式を使用します。

mpls label protocol ldp

no mpls label protocol ldp

構文の説明

LDP	LDP がインターフェイスで使用されるように指定します。

コマンド デフォルト

インターフェイスにプロトコルが明示的に設定されていない場合は、プラットフォームに設定された LDP が使用されます。プラットフォームの LDP を設定するには、**global mpls label protocol** コマンドを使用します。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 つのラベル スイッチ ルータ（LSR）を接続するリンクのラベル配布用のセッションを正常に確立するには、LSR のリンク インターフェイスが同じ LDP を使用するように設定されている必要があります。2 つの LSR を接続する複数のリンクがある場合は、2 つの LSR に接続しているすべてのリンク インターフェイスが同じプロトコルを使用するように設定されている必要があります。

次に、LDP をインターフェイスのラベル配布プロトコルとして確立する例を示します。

```
Switch(config-if)# mpls label protocol ldp
```

mpls label range

パケット インターフェイス上のマルチプロトコル ラベル スイッチング（MPLS）で使用できるローカル ラベルの範囲を設定するには、グローバル コンフィギュレーション モードで **mpls label range** コマンドを使用します。プラットフォームをデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

mpls label range *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*]

no mpls label range

構文の説明

minimum-value	ラベル スペースで許容される最小のラベルの値。デフォルトは 16 です。
maximum-value	ラベル スペースで許容される最大のラベルの値。デフォルトはプラットフォームによって異なります。
static	（任意）スタティック ラベル割り当てに使用するローカル ラベルのブロックを予約します。**static** キーワードと *minimum-static-valuemaximum-static-value* 引数を省略すると、スタティック割り当て用にラベルは予約されません。
minimum-static-value	（任意）スタティック ラベル割り当ての最小値。デフォルト値はありません。
maximum-static-value	（任意）スタティック ラベル割り当ての最大値。デフォルト値はありません。

コマンド デフォルト

プラットフォームのデフォルト値が使用されます。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ラベル 0 ~ 15 は IETF によって予約されており（詳細については、RFC 3032「MPLS Label Stack Encoding」を参照）、**mpls label range** コマンドで指定する範囲に含めることはできません。コマンドに 0 を入力すると、コマンドが認識されなかったコマンドであることを示すメッセージが表示されます。

mpls label range コマンドで定義されたラベル範囲は、（ダイナミック ラベル スイッチング、MPLS、MPLS トラフィック エンジニアリング、MPLS バーチャル プライベート ネットワーク（VPN）などの）ローカル ラベルを割り当てるすべての MPLS アプリケーションによって使用されます。

Label Distribution Protocol（LDP; ラベル配布プロトコル）などのラベル配布プロトコルを使用して、16 ～ 1048575 の汎用的なラベル範囲をダイナミック割り当て用に予約できます。

スタティック割り当て用にラベルを予約するには、オプションの **static** キーワードを指定します。MPLS スタティック ラベル機能では、スタティック割り当て用のラベルの範囲を設定する必要があります。スタティック バインディングは現在のスタティック範囲からのみ設定できます。スタティック範囲が設定されていないか、使い果たされている場合は、スタティック バインディングを設定できません。

ラベル値の範囲は、16 ～ 4096 です。最大値のデフォルトは、4096 です。たとえば、スタティック ラベル スペースを 16 ~ 100、ダイナミック ラベル スペースを 101 ～ 4096 のように分割することができます。

最小スタティック ラベル値の上限と下限がヘルプラインに表示されます。たとえば、ダイナミック ラベルの最小値を 16、最大値を 100 に設定すると、ヘルプ ラインには次のように表示されます。

```
Switch(config)# mpls label range 16 100 static ?
<100>  Upper Minimum static label value
<16>         Lower Minimum static label value
Reserved Label Range  --> 0    to 15
Available Label Range --> 16   to 4096
Static Label Range    --> 16   to 100
Dynamic Label Range   --> 101  to 4096
```

この例では、スタティックを 16 ～ 100 に設定できます。

下部の最小スタティック ラベル スペースが使用できない場合、最小値の下限はヘルプ ラインに表示されません。次に例を示します。

```
Switch(config)# mpls label range 16 100 static ?
  <16-100>  static label value range
```

次に、ローカルラベルスペースのサイズを設定する例を示します。この例では、最小スタティック値が 200 に、最大スタティック値が 4000 に設定されています。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# mpls label range 200 4000
Switch(config)#
```

現在の範囲に重複する新しい範囲を指定すると（たとえば、新しい範囲の最小スタティック値を 16、最大スタティック値を 1000 に設定する）、新しい範囲が即座に有効になります。

次に、ダイナミック ローカル ラベル スペースの最小スタティック値を 100、最大スタティック値を 1000 に設定し、スタティック ラベル スペースの最小スタティック値を 16、最大スタティック値を 99 に設定する例を示します。

```
Switch(config)# mpls label range 100 1000 static 16 99
Switch(config)#
```

リロード後に実行される **show mpls label range** コマンドの次の出力では、設定された範囲が有効になっていることが示されます。

```
Switch# show mpls label range
Downstream label pool: Min/Max label: 100/1000
Range for static labels: Min/Max/Number: 16/99
```

次に、ラベル範囲をデフォルト値に戻す例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no mpls label range
Switch(config)# end
```

関連コマンド

コマンド	説明
show mpls label range	MPLS ローカル ラベル スペースの範囲を表示します。

show mpls label range

パケットインターフェイスで使用可能なローカル ラベルの範囲を表示するには、特権 EXEC モードで **show mpls label range** コマンドを使用します。

show mpls label range

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

mpls label range コマンドを使用して、デフォルトの範囲とは異なるローカル ラベルの範囲を設定できます。**show mpls label range** コマンドでは、現在使用中のラベル範囲と、スイッチの次のリロード後に使用されるラベル範囲の両方が表示されます。

次に、最初のラベル範囲にオーバーラップしないラベル範囲を設定するために **mpls label range** コマンドを使用する前と後で、 **show mpls label range** コマンドを使用した場合の出力例を示します。

```
Switch# show mpls label range
Downstream label pool: Min/Max label: 16/100
Switch# configure terminal
Switch(config)# mpls label range 101 4000
Switch(config)# exit
Switch# show mpls label range
Downstream label pool: Min/Max label: 101/4000
```

関連コマンド

コマンド	説明
mpls label range	ローカル ラベルとして使用する値の範囲を設定します。

第 XII 部

マルチキャスト VPN（MVPN）

- マルチキャスト VPN，727 ページ

第 13 章

マルチキャスト VPN

- ip multicast-routing, 727 ページ
- ip multicast mrinfo-filter, 729 ページ
- mdt data, 730 ページ
- mdt default, 732 ページ
- mdt log-reuse, 733 ページ
- show ip pim mdt bgp, 734 ページ
- show ip pim mdt history, 736 ページ
- show ip pim mdt receive, 737 ページ
- show ip pim mdt send, 739 ページ

ip multicast-routing

IP マルチキャスト ルーティングを有効にするには、グローバル コンフィギュレーション モードで **ipmulticast-routing** コマンドを使用します。IP マルチキャスト ルーティングを無効にするには、このコマンドの **no** 形式を使用します。

ip multicast-routing [**vrf** *vrf-name*]

no ip multicast-routing [**vrf** *vrf-name*]

構文の説明

vrf*vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト VPN ルーティングおよび転送（MVRF）インスタンスのための IP マルチキャスト ルーティングを有効にします。

コマンド デフォルト

IP マルチキャスト ルーティングはディセーブルになっています。

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	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 マルチキャスト ルーティングがディセーブルになっている場合、Cisco IOS ソフトウェアはどのマルチキャスト パケットも転送しません。

（注） IPマルチキャストの場合は、IP マルチキャスト ルーティングを有効にした後に、PIM をすべてのインターフェイスに設定する必要があります。IP マルチキャスト ルーティングを無効にしても PIM は削除されません。PIM は、インターフェイスの設定から明示的に削除する必要があります。

次に、IP マルチキャスト ルーティングをイネーブルにする例を示します。

```
Switch(config)# ip multicast-routing
```

次に、特定の VRF の IP マルチキャスト ルーティングを有効にする例を示します。

```
Switch(config)#
ip multicast-routing vrf vrf1
```

次に、IP マルチキャスト ルーティングをディセーブルにする例を示します。

```
Switch(config)#
no ip multicast-routing
```

次に、Cisco IOS XE リリース 3.3S で特定の VRF の MDS を有効にする例を示します。

```
Switch(config)#
ip multicast-routing vrf vrf1
```

関連コマンド

コマンド	説明
ippim	インターフェイスに対して PIM をイネーブルにします。

ip multicast mrinfo-filter

マルチキャスト ルータ情報（mrinfo）要求パケットをフィルタ処理するには、グローバル コンフィギュレーション モードで **ipmulticastmrinfo-filter** コマンドを使用します。mrinfo 要求のフィルタを削除するには、このコマンドの **no** 形式を使用します。

ip multicast [**vrf** *vrf-name*] **mrinfo-filter** *access-list*

no ip multicast [**vrf** *vrf-name*] **mrinfo-filter**

構文の説明

vrf	（任意）VPN ルーティングおよび転送（VRF）インスタンスをサポートします。
vrf-name	（任意）VRF に割り当てられた名前。
access-list	どのネットワークまたはホストが **mrinfo** コマンドを使用して、ローカル マルチキャスト デバイスをクエリできるかを判別する IP 標準の番号付けまたは名前付けされたアクセス リスト。

コマンド デフォルト

デフォルトの動作または値はありません。

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
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

ipmulticastmrinfo-filter コマンドは、指定されたアクセス リストによって拒否されたすべての送信元からの mrinfo 要求パケットをフィルタ処理します。つまり、アクセス リストが送信元を拒否すると、その送信元の mrinfo 要求は除外されます。ACL によって許可された送信元からの mrinfo 要求は処理が許可されます。

次に、ネットワーク 192.168.1.1 のすべてのホストからの mrinfo 要求パケットをフィルタ処理し、その他のホストからの要求は許可する例を示します。

```
ip multicast mrinfo-filter 51
access-list 51 deny 192.168.1.1
access list 51 permit any
```

関連コマンド

コマンド	説明
mrinfo	ピアリングしている隣接するマルチキャストデバイスについて、マルチキャストデバイスにクエリします。

mdt data

データ マルチキャスト配信ツリー（MDT）プールで使用されるアドレス範囲を指定するには、VRF コンフィギュレーション モードまたは VRF アドレス ファミリ コンフィギュレーション モードで **mdtdata** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdt data threshold *kb/s*

no mdt data threshold *kb/s*

構文の説明

threshold*kb/s*	（任意）帯域幅しきい値をキロビット/秒（kb/s）単位で定義します。範囲は 1 ～ 4294967 です。

コマンド デフォルト

データ MDT プールは設定されていません。

コマンド モード

VRF アドレス ファミリ コンフィギュレーション（config-vrf-af）

VRF コンフィギュレーション（config-vrf）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

データ MDT には、MVPN ごとに最大 256 のマルチキャスト グループを含めることができます。データ MDT の作成に使用されるマルチキャスト グループは、設定済み IP アドレスのプールからダイナミックに選択されます。

データ MDT プールで使用されるアドレス範囲を指定するには、**mdtdata** コマンドを使用します。しきい値は、kb/s 単位で指定されます。オプションの **list** キーワードと *access-list* 引数を使用して、データ MDT プールで使用する (S, G) MVPN エントリを定義できます。これによって、データ MDT プールの作成は、*access-list* 引数に指定されたアクセス リストで定義された特定の (S, G) MVPN エントリにさらに限定されます。

mdtdata コマンドには、**ipvrf** 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できます。また、**mdtdata** コマンドには、**vrfdefinition** グローバル コンフィギュレーション コマンドに続けて **address-familyipv4** VRF コンフィギュレーション コマンドを使用することでもアクセスできます。

次に、MDT データ プールのグループ アドレスの範囲を設定する例を示します。500 kb/s のしきい値が設定されています。つまり、マルチキャスト ストリームが 1 kb/s を超えると、データ MDT が作成されます。

```
ip vrf vrf1
 rd 1000:1
 route-target export 10:27
 route-target import 10:27
 mdt default 236.1.1.1
 mdt data 228.0.0.0 0.0.0.127 threshold 500 list 101
!
.
.
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

関連コマンド

コマンド	説明
mdtdefault	VPN VRF のデフォルトの MDT グループを設定します。

mdt default

バーチャルプライベートネットワーク（VPN）ルーティングおよび転送（VRF）のデフォルトのマルチキャスト配信ツリー（MDT）グループを設定するには、VRF コンフィギュレーションまたは VRF アドレス ファミリ コンフィギュレーション モードで **mdtdefault** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

mdt default*group-address*

no mdt default*group-address*

構文の説明

group-address	デフォルト MDT グループの IP アドレス同じグループアドレスで設定されるプロバイダーエッジ（PE）デバイスはグループのメンバーになるため、このアドレスはコミュニティの ID として機能し、これによってプロバイダーエッジルータ間で相互にパケットを送受信できるようになります。

コマンド デフォルト

このコマンドはディセーブルです。

コマンド モード

VRF アドレス ファミリ コンフィギュレーション（config-vrf-af）VRF コンフィギュレーション（config-vrf）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	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 MDT グループは、同じ VPN に属するすべての PE デバイスに設定された同じグループである必要があります。

Source Specific Multicast（SSM; 送信元特定マルチキャスト）がデフォルト MDT のプロトコルとして使用されている場合、送信元 IP アドレスは、Border Gateway Protocol（BGP）セッションの送信元に使用されるアドレスです。

このコマンドによって、トンネル インターフェイスが作成されます。デフォルトでは、トンネルヘッダーの宛先アドレスは、 *group-address* 引数です。

mdtdefault コマンドには、**ipvrf** 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できます。また、**mdtdefault** コマンドには、**vrfdefinition** グローバル コンフィギュレーション コマンドに続けて **address-familyipv4** VRF コンフィギュレーション コマンドを使用することでもアクセスできます。

次に、Protocol Independent Multicast（PIM）SSM をバックボーンに設定する例を示します。そのため、デフォルト グループとデータ MDT グループは、IP アドレスの SSM 範囲内に設定されています。VPN の内部では、PIM スパースモード（PIM-SM）が設定され、Auto-RP アナウンスのみが受け入れられます。

```
ip vrf vrf1
 rd 1000:1
 mdt default 236.1.1.1
 mdt data 228.0.0.0 0.0.0.127 threshold 50
 mdt data threshold 50
 route-target export 1000:1
 route-target import 1000:1
!
!
```

関連コマンド

コマンド	説明
mdtdata	データ MDT グループ用にマルチキャスト グループのアドレス範囲を設定します。

mdt log-reuse

データ マルチキャスト配信ツリー（MDT）の再利用の記録を有効にするには、VRF コンフィギュレーション モードまたは VRF アドレス ファミリ コンフィギュレーション モードで **mdtlog-reuse** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

mdt log-reuse

no mdt log-reuse

構文の説明

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

このコマンドはディセーブルです。

コマンド モード

VRF アドレス ファミリ コンフィギュレーション（config-vrf-af）VRF コンフィギュレーション（config-vrf）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

mdtlog-reuse コマンドは、データ MDT が再利用されるたびに Syslog メッセージを生成します。

mdtlog-reuse コマンドには、**ipvrf** 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できます。また、**mdtlog-reuse** コマンドには、**vrfdefinition** グローバル コンフィギュレーション コマンドに続けて **address-familyipv4** VRF コンフィギュレーション コマンドを使用することでもアクセスできます。

次に、MDT の再利用のログを有効にする例を示します。

```
mdt log-reuse
```

関連コマンド

コマンド	説明
mdtdata	データ MDT グループ用にマルチキャスト グループのアドレス範囲を設定します。
mdtdefault	VPN VRF のデフォルトの MDT グループを設定します。

show ip pim mdt bgp

マルチキャスト配信ツリー（MDT）のデフォルト グループのルート識別子（RD）の Border Gateway Protocol（BGP）アドバタイズメントに関する詳細を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show ip pim mdt bgp コマンドを使用します。

show ip pim [**vrf** *vrf-name*] **mdt bgp**

構文の説明

vrf*vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスに関連付けられた MDT デフォルト グループの RD の BGP アドバタイズメントに関する情報を表示します。

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
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

MDT デフォルト グループの RD の詳細な BGP アドバタイズメントを表示するには、このコマンドを使用します。

次に、**showippimmdtbgp** コマンドの出力例を示します。

```
Device# show ip pim mdt bgp
MDT-default group 232.2.1.4
 rid:10.1.1.1 next_hop:10.1.1.1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *28*：*show ip pim mdt bgp* のフィールドの説明

フィールド	説明
MDT-default group	このルータにアドバタイズされた MDT デフォルト グループ。
rid:10.1.1.1	アドバタイズしたルータの BGP ルータ ID。
next_hop:10.1.1.1	アドバタイズメントに含まれていた BGP ネクスト ホップ アドレス。

show ip pim mdt history

再利用されているデータ マルチキャスト配信ツリー（MDT）グループの履歴に関する情報を表示するには、特権 EXEC モードで **showippimmdthistory** コマンドを使用します。

show ip pim vrf *vrf-name* **mdt history interval** *minutes*

構文の説明

vrf*vrf-name*	*vrf-name* 引数に指定されたマルチキャスト VPN（MVPN）ルーティングおよび転送（MVRF）インスタンス用に再利用されているデータ MDT グループの履歴を表示します。
interval*minutes*	再利用されているデータ MDT グループの履歴について情報を表示する間隔（分単位）を指定します。範囲は 1 ～ 71512 分（7 週間）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
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

showippimmdthistory コマンドの出力には、**interval** キーワードと *minutes* 引数で指定された間隔の再利用された MDT データ グループの履歴が表示されます。間隔は過去から現在まで、つまり、*minutes* 引数に指定された時間からコマンドが実行された時間までです。

次に、**showippimmdthistory** コマンドの出力例を示します。

```
Device# show ip pim vrf vrf1 mdt history interval 20
   MDT-data send history for VRF - vrf1 for the past 20 minutes
MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *29* : *show ip pim mdt history* のフィールドの説明

フィールド	説明
MDT-data group	情報が表示されている MDT データ グループ。
Number of reuse	このグループで再利用されたデータ MDT の数。

show ip pim mdt receive

プロバイダーエッジ（PE）ルータから受信したデータ マルチキャスト配信ツリー（MDT）グループ マッピングを表示するには、特権 EXEC モードで **showippimmdtreceive** コマンドを使用します。

show ip pim vrf *vrf-name* **mdt receive [detail]**

構文の説明

vrf*vrf-name*	*vrf-name* 引数に指定されたマルチキャスト VPN（MVPN）ルーティングおよび転送（MVRF）インスタンスのデータ MDT マッピングを表示します。
detail	（任意）受信されたデータ MDT アドバタイズメントの詳細な説明を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

ルータがデフォルトの MDT からデータ MDT に切り替えるときには、VRF 送信元、グループ ペア、およびトラフィックが送信されるグローバル マルチキャスト アドレスをアドバタイズしま

す。リモート ルータがこのデータを受信する場合は、このグローバル アドレス マルチキャスト グループに加入します。

次に、さらに情報を取得するために **detail** キーワードを使用した **showippimmdtreceive** コマンドの出力例を示します。

```
Device# show ip pim vrf vpn8 mdt receive detail
Joined MDT-data groups for VRF:vpn8
group:172.16.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *30*：*show ip pim mdt receive* のフィールドの説明

フィールド	説明
group:172.16.8.0	データ MDT を作成したグループ
source:10.0.0.100	データ MDT を作成した VRF 送信元
ref_count:13	このデータ MDT を再利用している (S, G) ペアの数。
OIF count:1	このマルチキャスト データを転送しているインターフェイスの数

フィールド	説明
flags:	エントリに関する情報です。 • A：候補となる Multicast Source Discovery Protocol（MSDP）アドバタイズメント • B：双方向グループ • D：デンス • C：接続済み • F：登録フラグ • I：受信した送信元固有のホスト レポート • J：最短パス送信元ツリー（SPT）の結合 • L：ローカル • M：MSDP が作成したエントリ • P：プルーニング済み • R：RP ビットが設定済み • S：スパース • s：Source Specific Multicast（SSM）グループ • T：SPT ビット セット • X：プロキシ結合タイマーの実行中 • U：URL Rendezvous Directory（URD） • Y：結合された MDT データ グループ • y：MDT データ グループに送信中 • Z：マルチキャスト トンネル

show ip pim mdt send

使用中のデータ マルチキャスト配信ツリー（MDT）グループを表示するには、特権EXECモードで **showippimmdtsend** コマンドを使用します。

show ip pim vrf *vrf-name* **mdt send**

構文の説明

vrf*vrf-name*	*vrf-name* 引数に指定されたマルチキャスト VPN（MVPN）ルーティングおよび転送（MVRF）インスタンスによって使用されているデータ MDT グループを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	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 MVRF によって使用されているデータ MDT グループを表示するには、このコマンドを使用します。

次に、**showippimmdtsend** コマンドの出力例を示します。

```
Device# show ip pim vrf vpn8 mdt send
MDT-data send list for VRF:vpn8
  (source, group)                      MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)             232.2.8.0           1
  (10.100.8.10, 225.1.8.2)             232.2.8.1           1
  (10.100.8.10, 225.1.8.3)             232.2.8.2           1
  (10.100.8.10, 225.1.8.4)             232.2.8.3           1
  (10.100.8.10, 225.1.8.5)             232.2.8.4           1
  (10.100.8.10, 225.1.8.6)             232.2.8.5           1
  (10.100.8.10, 225.1.8.7)             232.2.8.6           1
  (10.100.8.10, 225.1.8.8)             232.2.8.7           1
  (10.100.8.10, 225.1.8.9)             232.2.8.8           1
  (10.100.8.10, 225.1.8.10)            232.2.8.9           1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *31*：*show ip pim mdt send* のフィールドの説明

フィールド	説明
source, group	このルータがデータ MDT に切り替えた送信元とグループのアドレス
MDT-data group	これらのデータ MDT が送信されるマルチキャスト アドレス

フィールド	説明
ref_count	このデータ MDT を再利用している (S, G) ペアの数。

第 XIII 部

Network Management

- ネットワーク管理コマンド，745 ページ

第 14 章

ネットワーク管理コマンド

- description（ERSPAN），747 ページ
- destination（ERSPAN），748 ページ
- erspan-id，750 ページ
- filter（ERSPAN），751 ページ
- ip ttl（ERSPAN），752 ページ
- ip wccp，753 ページ
- monitor capture (interface/control plane)，756 ページ
- monitor capture buffer，760 ページ
- monitor capture clear，761 ページ
- monitor capture export，762 ページ
- monitor capture file，763 ページ
- monitor capture limit，765 ページ
- monitor capture match，766 ページ
- monitor capture start，767 ページ
- monitor capture stop，768 ページ
- monitor session，769 ページ
- monitor session destination，770 ページ
- monitor session filter，775 ページ
- monitor session source，777 ページ
- monitor session type erspan-source，780 ページ
- origin，781 ページ

- show ip sla statistics, 783 ページ
- show capability feature monitor, 784 ページ
- show monitor, 785 ページ
- show monitor capture, 788 ページ
- show monitor session, 789 ページ
- show platform ip wccp, 791 ページ
- show platform software swspan , 792 ページ
- snmp-server enable traps, 794 ページ
- snmp-server enable traps bridge, 798 ページ
- snmp-server enable traps bulkstat, 799 ページ
- snmp-server enable traps call-home, 800 ページ
- snmp-server enable traps cef, 801 ページ
- snmp-server enable traps cpu, 802 ページ
- snmp-server enable traps envmon, 803 ページ
- snmp-server enable traps errdisable, 804 ページ
- snmp-server enable traps flash, 805 ページ
- snmp-server enable traps isis, 806 ページ
- snmp-server enable traps license, 807 ページ
- snmp-server enable traps mac-notification, 808 ページ
- snmp-server enable traps ospf, 809 ページ
- snmp-server enable traps pim, 811 ページ
- snmp-server enable traps port-security, 812 ページ
- snmp-server enable traps power-ethernet, 813 ページ
- snmp-server enable traps snmp, 814 ページ
- snmp-server enable traps stackwise, 815 ページ
- snmp-server enable traps storm-control, 818 ページ
- snmp-server enable traps stpx, 819 ページ
- snmp-server enable traps transceiver, 820 ページ
- snmp-server enable traps vrfmib, 821 ページ
- snmp-server enable traps vstack, 822 ページ
- snmp-server engineID, 823 ページ

- snmp-server host, 824 ページ
- source（ERSPAN）, 828 ページ
- switchport mode access, 830 ページ
- switchport voice vlan, 830 ページ

description（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションを説明するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **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。

description *description*

no description

構文の説明

説明	このセッションのプロパティについて説明します。

コマンド デフォルト

説明は設定されていません。

コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

description 引数は 240 文字以内で指定します。

次に、ERSPAN 送信元セッションを説明する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# description source1
```

関連コマンド

コマンド	説明
monitorsessiontypeerspan-source	ローカルERSPAN送信元セッションを設定します。

destination（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションの宛先を設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **destination** コマンドを使用します。宛先セッションを削除するには、このコマンドの **no** 形式を使用します。

destination

no destination

構文の説明

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

送信元セッションの宛先は設定されていません。

コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ERSPAN トラフィックは、GRE カプセル化された SPAN トラフィックで、ERSPAN 宛先セッションによってだけ処理されます。

すべての ERSPAN 送信元セッション（最大 8）の宛先 IP アドレスが同一である必要はありません。ERSPAN 宛先セッションに IP アドレスを設定するには、**ipaddress** コマンドを入力します。

ERSPAN 送信元セッションの宛先 IP アドレスが（宛先スイッチ上のインターフェイスで設定される）、ERSPAN 宛先セッションが宛先ポートに送信するトラフィックの送信元です。**ipaddress** コマンドを使用して、送信元セッションおよび宛先セッションの両方に同一のアドレスを設定します。

次に、ERSPAN 送信元セッションの宛先を設定し、ERSPAN モニタ宛先セッション コンフィギュレーション モードを開始して、宛先プロパティを指定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)#ip address 10.1.1.1
Switch(config-mon-erspan-src-dst)#
```

次の **showmonitorsessionall** の出力例には、送信元セッションの宛先の異なる IP アドレスが示されています。

```
Switch# show monitor session all

Session 1
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session1
Destination IP Address : 10.1.1.1


Session 2
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session2
Destination IP Address : 192.0.2.1


Session 3
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session3
Destination IP Address : 198.51.100.1

Session 4
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session4
Destination IP Address : 203.0.113.1


Session 5
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session5
Destination IP Address : 209.165.200.225
```

関連コマンド

コマンド	説明
erspan-id	ERSPAN トラフィックを識別するため、宛先セッションで使用される ID を設定します。

コマンド	説明
ipttl	ERSPAN トラフィックのパケットの TTL 値を設定します。
monitorsessiontype erspan-source	ローカル ERSPAN 送信元セッションを設定します。
origin	ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。

erspan-id

Encapsulated Remote Switched Port Analyzer（ERSPAN）トラフィックを識別するために宛先セッションが使用する ID を設定するには、ERSPAN モニタ宛先セッション コンフィギュレーション モードで **erspan-id** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

erspan-id *erspan-ID*

no erspan-id *erspan-ID*

構文の説明

erspan-id	宛先セッションが使用する ERSPAN ID。有効値は 1 ～ 1023 です。

コマンド デフォルト

宛先セッションの ERSPAN ID は設定されていません。

コマンド モード

ERSPAN モニタ宛先セッション コンフィギュレーションモード（config-mon-erspan-src-dst）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、宛先セッションの ERSPAN ID を設定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
```

```
Switch(config-mon-erspan-src-dst)# erspan-id 3
```

関連コマンド

コマンド	説明
destination	ERSPAN宛先セッションを設定し、宛先プロパティを指定します。
monitorsessiontype erspan-source	ローカルERSPAN送信元セッションを設定します。

filter（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元がトランク ポートの場合に、ERSPAN 送信元 VLAN フィルタリングを設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで、**filter** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter {**ipaccess-group**{*standard-access-list*| *extended-access-list*| *acl-name*} | **ipv6access-group***acl-name*| **macaccess-group***acl-name*| **vlan***vlan-id*[**,**] [**-**]}

nofilter {**ip**[**access-group**| [*standard-access-list*| *extended-access-list*| *acl-name*]] | **ipv6**[**access-group**] | **mac**[**access-group**] | **vlan***vlan-id*[**,**] [**-**]}

構文の説明

ip	IP アクセス制御ルールを指定します。
access-group	アクセス制御グループを指定します。
standard-access-list	標準 IP アクセス リスト。
extended-access-list	拡張 IP アクセス リスト。
acl-name	アクセス リスト名。
ipv6	IPv6 アクセス制御ルールを指定します。
mac	Media Access Control（MAC）ルールを指定します。
vlan*vlan-ID*	ERSPAN 送信元 VLAN を指定します。有効な値は 1 ～ 4094 です。
,	（任意）別の VLAN を指定します。
-	（任意）VLAN の範囲を指定します。

コマンド デフォルト

送信元 VLAN フィルタリングは設定されていません。

コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 VLAN とフィルタ VLAN を同じセッションに含めることはできません。

モニタされたトランク インターフェイス上で **filter** コマンドを設定した場合、指定された VLAN セット上のトラフィックだけがモニタされます。

次に、送信元 VLAN フィルタリングを設定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# filter vlan 3
```

関連コマンド

コマンド	説明
monitorsessiontype erspan-source	ローカル ERSPAN 送信元セッションを設定します。

ip ttl（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）トラフィックのパケットの存続可能時間（TTL）を設定するには、ERSPAN モニタ宛先セッション コンフィギュレーション モードで **ipttl** コマンドを使用します。TTL 値を削除するには、このコマンドの **no** 形式を使用します。

ip ttl *ttl-value*

no ip ttl *ttl-value*

構文の説明

ttl-value	TTL の値。有効値は 2 ～ 255 です。

コマンド デフォルト

TTL 値は 255 として設定されます。

コマンド モード

ERSPAN モニタ宛先セッション コンフィギュレーションモード（config-mon-erspan-src-dst）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、ERSPAN トラフィックの TTL 値を設定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# ip ttl 32
```

関連コマンド

コマンド	説明
destination	ERSPAN宛先セッションを設定し、宛先プロパティを指定します。
monitorsessiontype erspan-source	ローカルERSPAN送信元セッションを設定します。

ip wccp

Webキャッシュ サービスを有効にし、アプリケーション エンジンで定義されたダイナミック サービスに対応するサービス番号を指定するには、デバイスで **ip wccp** グローバル コンフィギュレーション コマンドを使用します。サービスを無効にするには、このコマンドの **no** 形式を使用します。

ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

no ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

構文の説明

web-cache	Web キャッシュ サービスを指定します（WCCP バージョン 1 とバージョン 2）。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 の範囲で指定できます。サービスの最大数（**web-cache** キーワードで指定する Web キャッシュ サービスを含む）は 256 です。
group-address *groupaddress*	（任意）サービス グループに参加するためにデバイスおよびアプリケーション エンジンが使用するマルチキャスト グループ アドレスを指定します。
group-list *access-list*	（任意）マルチキャスト グループ アドレスが使用されない場合、サービス グループに加入しているアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。
redirect-list *access-list*	（任意）ホストから特定のホストまたは特定のパケットのリダイレクト サービスを指定します。
password *encryption-number password*	（任意）暗号化番号を指定します。指定できる範囲は 0 ～ 7 です。暗号化しない場合は 0、独自の場合は 7 を使用します。また、7 文字以内でパスワード名を指定します。デバイスは、パスワードと MD5 認証値を組み合わせて、デバイスとアプリケーション エンジンとの接続にセキュリティを確保します。デフォルトでは、パスワードは設定されておらず、認証も実行されていません。

コマンド デフォルト

WCCP サービスがデバイスでイネーブルにされていません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

シスコ エクスプレス フォワーディング スイッチングがイネーブルのとき、WCCP の透過的キャッシングはネットワーク アドレス変換（NAT）をバイパスします。この状況に対処するには、発信方向で WCCP 透過キャッシュを設定し、コンテンツ エンジン インターフェイスで Cisco Express Forwarding スイッチングを有効にし、**ip wccp web-cache redirect out** コマンドを指定します。キャッシュに面するルータ インターフェイスで **ip wccp redirect exclude in** コマンドを指定し、内部インターフェイスの着信方向に WCCP を設定します。この設定は、そのインターフェイスに到着したパケットのリダイレクションを回避します。

サービス グループを設定するときにリダイレクト リストを含めることもできます。指定されたリダイレクト リストは、NAT（送信元）IP アドレスを含むパケットを拒否して、リダイレクションを阻止します。

このコマンドは、指定されたサービス番号または Web キャッシュ サービス名のサポートをイネーブルまたはディセーブルにするようデバイスに指示します。サービス番号は 0 ～ 254 の範囲で指定できます。サービス番号または名前がイネーブルになると、ルータはサービス グループの確立に参加できます。

no ip wccp コマンドが入力されると、デバイスはサービス グループへの参加を終了し、引き続きサービスが設定されているインターフェイスがなければ領域の割り当てを解除し、他のサービスが設定されていなければ WCCP タスクを終了します。

web-cache に続くキーワードと *service-number* 引数はオプションで、任意の順序で指定できますが、1 回しか指定できません。

例

次に、Web キャッシュ、アプリケーション エンジンまたはサーバに接続されたインターフェイス、およびクライアントに接続するインターフェイスを設定する例を示します。

```
Device(config)# ip wccp web-cache
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no switchport
Device(config-if)# ip address 172.20.10.30 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)#
*Dec  6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

Device(config-if)# ip address 175.20.20.10 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# ip wccp web-cache group-listen
Device(config-if)# exit
```

関連トピック

show platform ip wccp, （791 ページ）

monitor capture (interface/control plane)

接続ポイントおよびパケット フロー方向を指定してモニタ キャプチャ ポイントを設定する、またはキャプチャ ポイントに接続ポイントを追加するには、特権 EXEC モードで **monitor capture** コマンドを使用します。指定した接続ポイントおよびパケットフロー方向でモニタ キャプチャを無効にする、またはキャプチャ ポイント上の複数の接続ポイントのいずれかを無効にするには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} {**interface** *interface-type interface-id* | **control-plane**} {**in** | **out** | **both**}

no monitor capture {*capture-name*} {**interface** *interface-type interface-id* | **control-plane**} {**in** | **out** | **both**}

構文の説明

capture-name	定義するキャプチャの名前。
interface *interface-type interface-id*	*interface-type* および *interface-id* とのインターフェイスを接続ポイントとして指定します。引数の意味は次のとおりです。 • **GigabitEthernet** *interface-id*：ギガビット イーサネット IEEE 802.3z インターフェイス。 • **vlan** *vlan-id*：VLAN。*vlan-id*の範囲は 1 ～ 4095 です。 • **capwap** *capwap-id*：Control and Provisioning of Wireless Access Points（CAPWAP）トンネリング インターフェイスを指定します。接続ポイントとして使用できる CAPWAP トンネルのリストを表示するには、**show capwap summary** コマンドを使用します。 （注） これはワイヤレス キャプチャに使用できる唯一の接続ポイントです。このインターフェイスを接続ポイントとして使用している場合、同じキャプチャ ポイントで他のインターフェイス タイプを接続ポイントとして使用することはできません。
control-plane	コントロール プレーンを接続ポイントとして指定します。
in | **out** | **both**	キャプチャするトラフィックの方向を指定します。

コマンド デフォルト

Wireshark キャプチャ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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

接続ポイントがこのコマンドを使用してキャプチャ ポイントに関連付けられると、方向を変更する唯一の方法は、このコマンドの**no**形式を使用して接続ポイントを削除し、新しい方向に接続ポイントを再接続することです。接続ポイントの方向は上書きできません。

接続ポイントがキャプチャ ポイントから削除され、1 つの接続ポイントのみが関連付けられている場合、キャプチャ ポイントは効率的に削除されます。

このコマンドを別の接続ポイントで再実行することで、複数の接続ポイントをキャプチャ ポイントと関連付けることができます。次に例を示します。

複数のキャプチャ ポイントを定義できますが、一度にアクティブにできるのは 1 つだけです。つまり、1 つ開始するには 1 つ停止する必要があります。

インターフェイスの出力方向にキャプチャされたパケットは、スイッチの書き換えによって行われた変更（TTL、VLAN タグ CoS、チェックサム、および MAC アドレス、DSCP、プレシデント、UP など）が反映されないこともあります。

特定の順序はキャプチャ ポイントを定義する場合には適用されません。任意の順序でキャプチャ ポイント パラメータを定義できます。Wireshark CLI では、単一行のパラメータ数に制限はありません。これはキャプチャ ポイントを定義するために必要なコマンドの数を制限します。

VRF、管理ポート、プライベート VLAN はいずれも接続ポイントとして使用することはできません。

Wireshark は宛先 SPAN ポートでパケットをキャプチャできません。

VLAN が Wireshark の接続ポイントとして使用されている場合、パケットは、入力方向でのみキャプチャされます。

ワイヤレス（CAPWAP）使用上の注意事項

ワイヤレス キャプチャの唯一の形式は CAPWAP トンネル キャプチャです。

CAPWAP トンネルをキャプチャする場合、同じキャプチャ ポイント上で他のインターフェイス タイプを接続ポイントとして使用することはできません。また、同じキャプチャ ポイント上で可能な接続ポイントの唯一異なるタイプはコントロールプレーンです。コントロールプレーンおよび CAPWAP トンネル接続ポイントの組み合わせは、すべてのワイヤレス関連トラフィックをキャプチャできます。

複数の CAPWAP トンネルのキャプチャがサポートされています。各 CAPWAP トンネルの ACL は結合され、単一 ACL としてスイッチに送信されます。

コア フィルタは適用されず、CAPWAP トンネルをキャプチャする場合に省略できます。コントロール プレーンおよびCAPWAP トンネルが混在している場合、コア フィルタはコントロール プレーン パケットにも適用されません。

CAPWAP の非データ トンネルをキャプチャするには、管理 VLAN でトラフィックをキャプチャし、適切な ACL を適用してトラフィックをフィルタします。この ACL はコア フィルタ ACL と結合され、スイッチに単一の ACL として割り当てられることに注意してください。

例

物理インターフェイスを接続ポイントとして使用してキャプチャ ポイントを定義するには次を実行します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

（注） 2つ目のコマンドは、キャプチャ ポイントのコア フィルタを定義します。これは、キャプチャ ポイントでCAPWAP トンネリング接続ポイントを使用している場合を除いて、キャプチャ ポイントが機能するために必要です。

キャプチャ ポイントでCAPWAP トンネリング接続ポイントを使用している場合、コア フィルタを使用できません。

複数の接続ポイントを持つキャプチャ ポイントを定義するには次を実行します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap control-plane in
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
```

複数の接続ポイントで定義されたキャプチャ ポイントから接続ポイントを削除するには次を実行します。

```
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
Device# no monitor capture mycap control-plane
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
```

CAPWAP 接続ポイントでキャプチャ ポイントを定義するには次を実行します。

```
Device# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0


Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                 data Gi3/0/6   unicast   -


Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

Device# monitor capture mycap interface capwap 0 both
```

```
Device# monitor capture mycap file location flash:mycap.pcap
Device# monitor capture mycap file buffer-size 1
Device# monitor capture mycap start

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

Device# show monitor capture mycap parameter
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
Device#
Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
Device#
Device# show monitor capture file flash:mycap.pcap
  1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
```

```
24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
```

関連トピック

monitor capture buffer, （760 ページ）

monitor capture file, （763 ページ）

show monitor capture, （788 ページ）

monitor capture buffer

モニタ キャプチャ（WireShark）のバッファを設定するには、特権 EXEC モードで **monitor capture buffer** コマンドを使用します。モニタ キャプチャ バッファを無効にする、またはバッファを循環バッファからデフォルトの線形バッファに戻すには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **buffer** {**circular** [**size** *buffer-size*] | **size** *buffer-size*}

no monitor capture {*capture-name*} **buffer** [**circular**]

構文の説明

capture-name	バッファが設定されるキャプチャの名前。
circular	バッファが循環タイプであることを指定します。循環タイプのバッファは、バッファが消費された後も以前にキャプチャされたデータを上書きすることでデータのキャプチャを継続します。
size *buffer-size*	（任意）バッファのサイズを指定します。範囲は 1 ～ 100 MB です。

コマンド デフォルト

線形バッファが設定されます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

最初に WireShark のキャプチャを設定すると、小規模の循環バッファが提案されます。

例

1 MB のサイズの循環バッファを設定する場合は次を実行します。

```
Device# monitor capture mycap buffer circular size 1
```

関連トピック

monitor capture (interface/control plane), （756 ページ）

monitor capture file, （763 ページ）

show monitor capture, （788 ページ）

monitor capture clear

モニタ キャプチャ（WireShark）バッファをクリアするには、特権 EXEC モードで **monitor capture clear** コマンドを使用します。

monitor capture {*capture-name*} **clear**

構文の説明

capture-name	バッファがクリアされるキャプチャの名前。

コマンド デフォルト

バッファのコンテンツはクリアされません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

キャプチャ中、または 1 つ以上の最終条件が満たされたか **monitor capture stop** コマンドを入力したためにキャプチャが停止された後に、**monitor capture clear** コマンドを使用します。キャプチャが停止した後に **monitor capture clear** コマンドを入力した場合、バッファにキャプチャされたパケットがないため、ファイルへのキャプチャされたパケットのコンテンツの保存に使用された **monitor capture export** コマンドには影響はありません。

パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。

例

mycap をキャプチャするためにバッファ コンテンツをクリアするには次を実行します。

```
Device#  monitor capture mycap clear
```

monitor capture export

ファイルにモニタ キャプチャ（WireShark）をエクスポートするには、特権 EXEC モードで **monitor capture export** コマンドを使用します。

monitor capture {*capture-name*} **export** *file-location* : *file-name*

構文の説明

capture-name	エクスポートするキャプチャの名前。
file-location : *file-name*	（任意）キャプチャ ストレージ ファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。 • flash：オンボード フラッシュ ストレージ • (usbflash0:)：USB ドライブ

コマンド デフォルト

キャプチャされたパケッ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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

ストレージの宛先がキャプチャ バッファである場合にのみ **monitor capture export** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。キャプチャ中またはパケット キャプチャ停止後にこのコマンドを使用します。パケット キャプチャは、1 つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireShark がスタック内のスイッチで使用される場合、パケット キャプチャは前述の *file-location* で指定されたアクティブ スイッチに接続されるデバイス上にのみ保存されます。例：flash1 はアクティブなスイッチに接続されています。flash2 はセカンダリ スイッチに接続されています。この場合、パケット キャプチャの保存に使用できるのは flash1 だけです。

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

例

キャプチャ バッファの内容を flash ドライブの mycap.pcap にエクスポートするには次を実行します。

```
Device# monitor capture mycap export flash:mycap.pcap
```

monitor capture file

モニタ キャプチャ（WireShark）ストレージ ファイル属性を設定するには、特権 EXEC モードで **monitor capture file** コマンドを使用します。ストレージ ファイル属性を削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **file**{[**buffer-size** *temp-buffer-size*][**location** *file-location* : *file-name*][**ring** *number-of-ring-files*][**size** *total-size*]}

no monitor capture {*capture-name*} **file**{[**buffer-size**][**location**][**ring**][**size**]}

構文の説明

capture-name	変更するキャプチャの名前。

buffer-size *temp-buffer-size*	（任意）一時バッファのサイズを指定します。*temp-buffer-size* の範囲は 1 ～ 100 MB です。これはパケット損失を削減するために指定されます。
location *file-location* : *file-name*	（任意）キャプチャ ストレージファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。 • flash：オンボード フラッシュ ストレージ • (usbflash0:)：USB ドライブ
ring *number-of-ring-files*	（任意）キャプチャが循環ファイル チェーンに保存されること、およびファイル リング内のファイル数を指定します。
size *total-size*	（任意）キャプチャ ファイルの合計サイズを指定します。

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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

ストレージの宛先がファイルである場合にのみ **monitor capture file** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。パケット キャプチャの停止後にこのコマンドを使用します。パケット キャプチャは、1 つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireShark がスタック内のスイッチで使用される場合、パケット キャプチャは前述の *file-location* で指定されたアクティブ スイッチに接続されるデバイス上にのみ保存されます。例：flash1 はアクティブなスイッチに接続されています。flash2 はセカンダリ スイッチに接続されています。この場合、パケット キャプチャの保存に使用できるのは flash1 だけです。

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

例

フラッシュ ドライブに保管されているファイル名が mycap.pcap であることを指定するには次を実行します。

```
Device# monitor capture mycap file location flash:mycap.pcap
```

関連トピック

monitor capture (interface/control plane), （756 ページ）

monitor capture buffer, （760 ページ）

show monitor capture, （788 ページ）

monitor capture limit

キャプチャ制限を設定するには、特権 EXEC モードで **monitor capture limit** コマンドを使用します。キャプチャ制限を削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]}

no monitor capture {*capture-name*} **limit** [**duration**][**packet-length**][**packets**]

構文の説明

capture-name	キャプチャ制限を割り当てられるキャプチャの名前。
duration*seconds*	（任意）キャプチャ期間（秒）を指定します。範囲は 1 ～ 1000000 です。
packet-length*size*	（任意）パケット長（バイト）を指定します。実際のパケットが特定の長さより長い場合、数がバイト引数によって示される最初のセットのバイトのみが保存されます。
packets*num*	（任意）キャプチャに対して処理されるパケット数を指定します。

コマンド デフォルト

キャプチャ制限は設定されません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

60 秒のセッション制限および 400 バイトのパケット セグメント長を設定するには次を実行します。

```
Device# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture match

（注） CAPWAP トンネルをキャプチャする場合は、このコマンドを使用しないでください。また、コントロール プレーンおよび CAPWAP トンネルが混在している場合、このコマンドには効果がありません。

モニタ（Wireshark）キャプチャに対して明示的にインライン コア フィルタを定義するには、特権 EXEC モードで **monitor capture match** コマンドを使用します。このフィルタを削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}}

no monitor capture {*capture-name*} **match**

構文の説明

capture-name	コア フィルタを割り当てられるキャプチャの名前。
any	すべてのパケットを指定します。
mac*mac-match-string*	レイヤ 2 パケットを指定します。
ipv4	IPv4 パケットを指定します。
host	ホストを指定します。
protocol	プロトコルを指定します。
ipv6	IPv6 パケットを指定します。

コマンド デフォルト

特権 EXEC モードでは、フィルタは設定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

ソースまたは宛先上の任意の IP バージョン 4 パケットに一致するキャプチャ ポイントに対してキャプチャ ポイントおよびコア フィルタを定義するには、次を実行します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

monitor capture start

トラフィック トレース ポイントでパケット データのバッファへのキャプチャを開始するには、特権 EXEC モードで **monitor capture start** コマンドを使用します。

monitor capture {*capture-name*} **start**

構文の説明

capture-name	開始するキャプチャの名前。

コマンド デフォルト

バッファのコンテンツはクリアされません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

キャプチャ ポイントが定義された後にパケット データ キャプチャを有効にするには、**monitor capture clear** コマンドを使用します。パケット データのキャプチャを停止するには、**monitor capture stop** コマンドを使用します。

CPUおよびメモリなどのシステム リソースがキャプチャの開始前に使用可能であることを確認します。

例

バッファ コンテンツのキャプチャを開始するには次を実行します。

```
Device#  monitor capture mycap start
```

monitor capture stop

トラフィック トレース ポイントでパケット データのキャプチャを停止するには、特権EXECモードで **monitor capture stop** コマンドを使用します。

monitor capture {*capture-name*} **stop**

構文の説明

capture-name	停止するキャプチャの名前。

コマンド デフォルト

パケット データ キャプチャが進行中です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

monitor capture stop コマンドを使用して、**monitor capture start** コマンドによって開始したパケット データのキャプチャを停止します。線形および循環の 2 つのタイプのキャプチャ バッファを設定できます。線形バッファがいっぱいになった場合、データ キャプチャは自動的に停止します。循環バッファがいっぱいになると、データ キャプチャは最初から開始し、データは上書きされます。

例

バッファ コンテンツのキャプチャを停止するには次を実行します。

```
Device#  monitor capture mycap stop
```

monitor session

ポート間のトラフィック分析のために、イーサネット 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 スイッチド ポート アナライザ（RSPAN）セッションのコンフィギュレーションを新規作成するか、既存のセッションのコンフィギュレーションに追加するには、**monitor session** グローバル コンフィギュレーション コマンドを使用します。SPAN セッションまたは RSPAN セッションをクリアするには、このコマンドの **no** 形式を使用します。

monitor session *session-number* {**destination** | **filter** | **source**}

no monitor session {*session-number* [**destination** | **filter** | **source**] | **all** | **local** | **range** *session-range* | **remote**}

構文の説明

session-number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
all	すべてのモニタ セッションをクリアします。
local	すべてのローカル モニタ セッションをクリアします。
range *session-range*	指定された範囲のモニタ セッションをクリアします。
remote	すべてのリモート モニタ セッションをクリアします。

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

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、RSPAN、FSPAN、および FRSPAN の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。

例

次に、ローカル SPAN セッション 1 を作成して Po13（EtherChannel ポート）のトラフィックをモニタし、セッションの SPAN トラフィックを VLAN 1281 のみに限定する例を示します。出力トラフィックは送信元を複製します。入力転送はイネーブルになりません。

```
Device(config)# monitor session 1 source interface Po13
Device(config)# monitor session 1 filter vlan 1281
Device(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
 replicate
Device(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
 replicate
```

次に、これらのセットアップ手順を完了した後の **show monitor session all** コマンドの出力を示します。

```
Device# show monitor session all

Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Po13
Destination Ports      : Gi2/0/36,Gi3/0/36
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : 1281
...
```

関連トピック

monitor session destination, （770 ページ）

monitor session filter, （775 ページ）

monitor session source, （777 ページ）

show monitor, （785 ページ）

monitor session destination

新規にスイッチド ポート アナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）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 Sensor アプライアンスなど）の宛先ポート上の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を追加または削除するには、**monitor session destination** グローバル コンフィ

ギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから宛先インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

no monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

構文の説明

session-number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
interface*interface-id*	SPAN または RSPAN セッションの宛先または送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポート チャネルも有効なインターフェイス タイプであり、指定できる範囲は 1 ～ 128 です。
,	（任意）複数のインターフェイスまたは VLAN を指定します。または、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。
encapsulation replicate	（任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。**encapsulation** オプションは、**no** 形式では無視されます。

encapsulation dot1q	（任意）宛先インターフェイスが IEEE 802.1Q カプセル化の送信元インターフェイスの着信パケットを受け入れるように指定します。 次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。**encapsulation** オプションは、**no** 形式では無視されます。
ingress	入力トラフィック転送をイネーブルにします。
dot1q	（任意）指定された VLAN をデフォルト VLAN として、IEEE 802.1Q カプセル化された着信パケットを受け入れます。
untagged	（任意）指定された VLAN をデフォルト VLAN として、タグなしカプセル化された着信パケットを受け入れます。
isl	ISL カプセル化を使用して入力トラフィックを転送するように指定します。
remote	RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。
vlan*vlan-id*	**ingress** キーワードとのみ使用された場合、入力トラフィックに対するデフォルトの VLAN を設定します。

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。

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。

all、**local**、**range***session-range*、または **remote** を **no monitor session** コマンドとともに指定して、それぞれ SPAN と RSPAN セッションすべて、ローカル SPAN セッションすべて、一定範囲のセッション、RSPAN セッションすべてをクリアできます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

8 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

SPAN または RSPAN の宛先は物理ポートである必要があります。

スイッチ上またはスイッチ スタック上で、最大 64 の宛先ポートを保有できます。

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。[**,** | **-**] オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN 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。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。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1x 認証をイネーブルにすることはできますが、ポートが SPAN 宛先として削除されるまで IEEE 802.1x 認証はディセーブルです。IEEE 802.1x 認証がポート上で使用できない場合、スイッチはエラー メッセージを返します。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

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***destinationinterface***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** と **untagged** のいずれであるかによって決まります。
- その他のキーワードを指定せずに、**monitor session***session_number***destinationinterface***interface-id***encapsulationreplicate** 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***destinationinterface***interface-id***encapsulationreplicate 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 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** と **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）。

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、RSPAN、FSPAN、および FRSPAN の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。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
Device(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

次の例では、ある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。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination remote vlan 900
Device(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。

```
Device(config)# monitor session 10 source remote vlan 900
Device(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 dot1q 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。

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
 vlan 5
```

関連トピック

monitor session, （769 ページ）

monitor session filter, （775 ページ）

monitor session source, （777 ページ）

show monitor, （785 ページ）

monitor session filter

フローベース SPAN（FSPAN）セッションやフローベース RSPAN（FRSPAN）送信元または宛先セッションを新しく開始する、または特定の VLAN に対して SPAN 送信元トラフィックを制限（フィルタ処理）するには、**monitor session 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。SPAN または RSPAN セッションからフィルタを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }

no monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }

構文の説明

session-number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
vlan *vlan-id*	SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとして VLAN のリストを指定します。*vlan-id* で指定できる範囲は 1 ～ 4094 です。
,	任意）複数の VLAN を指定します。または VLAN 範囲を前の範囲から区切ります。カンマの前後にスペースを入れます。

-	（任意）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。

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

1 つの VLAN、または複数のポートや VLAN、特定範囲のポートや VLAN でトラフィックをモニタできます。複数または一定範囲の VLAN を指定するには、**[,** | **-]** オプションを使用します。

複数の VLAN 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 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。

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。

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、RSPAN、FSPAN、および FRSPAN の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。

例

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
```

次に、ローカル SPAN セッション 1 を作成してスタック メンバ 1 の送信元ポート 1 とスタック メンバ 2 の宛先ポートの送受信両方のトラフィックをモニタし、FSPAN セッションでアクセス リスト番号 122 を使用して IPv4 トラフィックをフィルタする例を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 1 filter ip access-group 122
```

関連トピック

monitor session, （769 ページ）

monitor session destination, （770 ページ）

monitor session source, （777 ページ）

show monitor, （785 ページ）

monitor session source

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）送信元セッションを開始する、または既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session source** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

no monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

構文の説明

session_number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
interface *interface-id*	SPAN または RSPAN セッションの送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポート チャネルも有効なインターフェイス タイプであり、指定できる範囲は 1 ～ 48 です。

,	（任意）複数のインターフェイスまたは VLAN を指定します。または、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。
both | **rx** | **tx**	（任意）モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。
remote	（任意）RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。
vlan *vlan-id*	**ingress** キーワードだけで使用された場合、入力トラフィックにデフォルトの VLAN を設定します。

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

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。

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。[**,** | **-**] オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN 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。

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 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。

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、RSPAN、FSPAN、および FRSPAN の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。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

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 gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

関連トピック

monitor session, （769 ページ）

monitor session destination, （770 ページ）

monitor session filter, （775 ページ）

show monitor, （785 ページ）

monitor session type erspan-source

ローカルの Encapsulated Remote Switched Port Analyzer（ERSPAN）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 **monitorsessiontypeerspan-source** コマンドを使用します。ERSPAN 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。

monitor session *span-session-number* **type erspan-source**

no monitor session *span-session-number* **type erspan-source**

構文の説明

span-session-number	ローカル ERSPAN セッションの番号。有効値は 1 ～ 66 です。

コマンド デフォルト

ERSPAN 送信元セッションは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

span-session-number およびセッション タイプ（*erspan-source* キーワードによって設定）は、設定後は変更できません。セッションを削除するには、このコマンドの **no** 形式を使用し、新しいセッション ID または新しいセッション タイプでセッションを再作成します。

ERSPAN 送信元セッションの宛先 IP アドレスが（宛先スイッチ上のインターフェイスで設定される必要がある）、ERSPAN 宛先セッションが宛先ポートに送信するトラフィックの送信元です。ERSPAN モニタ宛先セッション コンフィギュレーション モードで **ipaddress** コマンドを使用して、送信元セッションと宛先セッションの両方に同じアドレスを設定できます。

ERSPAN ID により、同じ宛先 IP アドレスに着信する ERSPAN トラフィックと異なる ERSPAN 送信元セッションとが区別されます。

ローカル ERSPAN 送信元セッションの最大数は 8 に制限されています。

次に、ERSPAN 送信元セッション番号を設定する例を示します。

```
Switch(config)# monitor session 55 type erspan-source
Switch(config-mon-erspan-src)#
```

関連コマンド

コマンド	説明
monitorsessiontype	ERSPAN送信元セッション番号を作成するか、セッションに対して ERSPAN セッション コンフィギュレーション モードを開始します。
showcapabilityfeaturemonitor	モニタ機能に関する情報を表示します。
showmonitorsession	ERSPAN、SPAN、RSPAN のセッションに関する情報を表示します。

origin

Encapsulated Remote Switched Port Analyzer（ERSPAN）トラフィックの送信元として使用する IP アドレスを設定するには、ERSPAN モニタ宛先セッション コンフィギュレーション モードで **origin** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

origin *ip-address*

no origin *ip-address*

構文の説明

ip-address	ERSPAN 送信元セッションの宛先 IP アドレスを指定します。

コマンド デフォルト

送信元 IP アドレスは設定されていません。

コマンド モード

ERSPAN モニタ宛先セッション コンフィギュレーションモード（config-mon-erspan-src-dst）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

スイッチの ERSPAN 送信元セッションは、**origin** コマンドを使用して、さまざまな送信元 IP アドレスを使用できます。

次に、ERSPAN 送信元セッションの IP アドレスを設定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# origin ip-address 203.0.113.2
```

次の **showmonitorsessionall** コマンドの出力例では、異なる送信元 IP アドレスの ERSPAN 送信元セッションが表示されます。

```
Session 3
---------
Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
Both : Gi1/0/13
Destination IP Address : 10.10.10.10
Origin IP Address : 10.10.10.10


Session 4
---------
Type : ERSPAN Source Session
Status : Admin Enabled
Destination IP Address : 192.0.2.1
Origin IP Address : 203.0.113.2
```

関連コマンド

コマンド	説明
destination	ERSPAN宛先セッションを設定し、宛先プロパティを指定します。
monitorsessiontype erspan-source	ローカルERSPAN送信元セッションを設定します。

show ip sla statistics

Cisco IOS IP サービス レベル契約（SLA）のすべての動作または指定された動作の現在または集約された動作ステータスおよび統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip sla statistics** コマンドを使用します。

show ip sla statistics [*operation-number* [**details**] | **aggregated** [*operation-number* | **details**] | **details**]

構文の説明

operation-number	（任意）動作ステータスおよび統計情報を表示する動作の番号。受け入れられる値の範囲は 1 ～ 2147483647 です。
details	（任意）詳細出力を指定します。
aggregated	（任意）IP SLA 集約統計を指定します。

コマンド デフォルト

稼働しているすべての IP SLA 動作の出力を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

動作の残りの継続時間、動作がアクティブかどうか、完了時刻など、IP SLA 動作の現在の状態を表示するには、**show ip sla statistics** を使用します。出力には、最後の（最近完了した）動作に対して返されたモニタリング データも含まれます。この生成された操作 ID は、基本マルチキャスト操作に対して、また操作全体の要約統計の一部として **show ip sla** コンフィギュレーション コマンドを使用すると表示されます。

あるレスポンダに関する詳細を表示するには、その特定の操作 ID に **show** コマンドを入力します。

例

次に、**show ip sla statistics** コマンドの出力例を示します。

```
Device# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show capability feature monitor

モニタ機能に関する情報を表示するには、特権 EXEC モードで **show capability feature monitor** コマンドを使用します。

show capabilityfeaturemonitor{**erspan-destination**| **erspan-source**}

構文の説明

erspan-destination	設定済みの Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションに関する情報を表示します。
erspan-source	すべての設定済みのグローバル組み込みテンプレートを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、**show capability feature monitor erspan-source** コマンドの出力例を示します。

```
Switch# show capability feature monitor erspan-source

ERSPAN Source Session Supported: true
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II
ACL filter Supported: true
Fragmentation Supported: true
Truncation Supported: false
Sequence number Supported: false
QOS Supported: true
```

次に、**show capability feature monitor erspan-destination** コマンドの出力例を示します。

```
Switch# show capability feature monitor erspan-destination

ERSPAN Destination Session Supported: false
```

関連コマンド

コマンド	説明
monitor session type erspan-source	ERSPAN送信元セッション番号を作成するか、セッションに対して ERSPAN セッション コンフィギュレーション モードを開始します。

show monitor

すべての Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）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。

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]]

構文の説明

session	（任意）指定されたSPANセッションの情報を表示します。

session_number	SPANまたはRSPANセッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
all	（任意）すべての SPAN セッションを表示します。
local	（任意）ローカル SPAN セッションだけを表示します。
range *list*	（任意）一定範囲のSPANセッションを表示します。*list* は有効なセッションの範囲です。range は単一のセッション、または2つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 （注） このキーワードは、特権 EXEC モードの場合だけ使用可能です。
remote	（任意）リモート SPAN セッションだけを表示します。
detail	（任意）指定されたセッションの詳細情報を表示します。

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
Cisco IOS XE 3.2SE	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 monitor コマンドと**show monitor session all** コマンドの出力は同じです。

SPAN 送信元セッションの最大数：2（送信元およびローカル セッションに適用）

例

次に、**show monitor** ユーザ EXEC コマンドの出力例を示します。

```
Device# show monitor
```

```
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力を示します。

```
Device# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all** ユーザ EXEC コマンドの出力を示します。

```
Device# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

関連トピック

monitor session, （769 ページ）

monitor session destination, （770 ページ）

monitor session filter, （775 ページ）

monitor session source, （777 ページ）

show monitor capture

モニタ キャプチャ（WireShark）の内容を表示するには、特権 EXEC モードで **show monitor capture file** コマンドを使用します。

show monitor capture [*capture-name* [**buffer**] | **file** *file-location* : *file-name*][**brief** | **detailed** | **display-filter** *display-filter-string*]

構文の説明

capture-name	（任意）表示するキャプチャの名前を指定します。
buffer	（任意）指定されたキャプチャに関連するバッファが表示されることを指定します。
file *file-location* : *file-name*	（任意）表示するキャプチャ ストレージ ファイルのファイル位置と名前を指定します。
brief	（任意）表示内容の概要を指定します。
detailed	（任意）詳細な表示内容を指定します。
display-filter *display-filter-string*	*display-filter-string* に従って表示内容をフィルタ処理します。

コマンド デフォルト

すべてのキャプチャの内容を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

mycap という名前のキャプチャのキャプチャを表示するには次を実行します。

```
Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

関連トピック

monitor capture (interface/control plane), （756 ページ）

monitor capture buffer, （760 ページ）

monitor capture file, （763 ページ）

show monitor session

すべての Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）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 session** コマンドを使用します。

show monitor session {*session_number* | **all** | **erspan-source** | **local** | **range** *list* | **remote**} [**detail**]

構文の説明

session_number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 68 です。ただし、このスイッチが Catalyst 2960-S スイッチとスタックされる場合、2 個のローカル 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に限定され、範囲は 1 ～ 66 になります。
all	すべての SPAN セッションを表示します。
erspan-source	送信元 ERSPAN セッションだけを表示します。

local	ローカル SPAN セッションだけを表示します。
range *list*	一定範囲の SPAN セッションを表示します。*list* は有効なセッションの範囲です。rangeは単一のセッション、または 2 つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 （注） このキーワードは、特権EXECモードの場合だけ使用可能です。
remote	リモート SPAN セッションだけを表示します。
detail	（任意）指定されたセッションの詳細情報を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

ローカルの ERSPAN 送信元セッションの最大数は 8 です。

例

次に、ローカル SPAN 送信元セッション 1 に対する **show monitor session** コマンドの出力例を示します。

```
Device# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次に、入力トラフィックの転送が有効になっている場合の **show monitor session all** コマンドの出力例を示します。

```
Device# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

次に、**show monitor session erspan-source** コマンドの出力例を示します。

```
Switch# show monitor session erspan-source

Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
RX Only : Gi1/4/33
Destination IP Address : 20.20.163.20
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IPv6 Flow Label : None
```

show platform ip wccp

プラットフォーム依存 Web Cache Communication Protocol（WCCP）情報を表示するには、**show platform ip wccp** 特権 EXEC コマンドを使用します。

show platform ip wccp {**cache-engines | interfaces | service-groups**}[**switch** *switch-number*]

構文の説明

cache-engines	WCCP キャッシュ エンジンを表示します。
interfaces	WCCP インターフェイスを表示します。
service-groups	WCCP サービス グループを表示します。
switch *switch-number*	（任意）指定された *switch-number* の WCCP 情報のみを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

このコマンドは、デバイスが IP サービス フィーチャ セットを実行している場合だけ使用可能です。

次に、WCCP インターフェイスを表示する例を示します。

```
Device# show platform ip wccp interfaces

WCCP Interfaces


**** WCCP Interface Gi1/0/3 iif_id:0x104a60000000087 (#SG:1), vrf:0 Ingress
le_handle:0x565dd208 IPv4 Sw-Label:3, Asic-Label:3

* Service group id:0 type: Well-known    token:126 vrf:0 (ref count:1)
Open service    prot: PROT_TCP  l4_type: Dest ports     priority: 240
port[0]: 80
```

関連トピック

ip wccp, （753 ページ）

show platform software swspan

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）情報を表示するには、特権 EXEC モードで **show platform software swspan** コマンドを使用します。

show platform software swspan {**switch**} {{{**F0**| **FP active**} **counters**}| **R0**| **RP active**} {**destinationsess-id***session-ID*| **sourcesess-id***session-ID*}

構文の説明

switch	スイッチに関する情報を表示します。
F0	Embedded Service Processor（ESP）スロット 0 に関する情報を表示します。
FP	ESP に関する情報を表示します。

active	ESP またはルート プロセッサ（RP）のアクティブ インスタンスに関する情報を表示します。
counters	SWSPAN メッセージ カウンタを表示します。
R0	RP スロット 0 に関する情報を表示します。
RP	RP に関する情報を表示します。
destinationsess-id*session-ID*	指定された宛先セッションに関する情報を表示します。
sourcesess-id*session-ID*	指定された送信元セッションに関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドは、Cisco IOS Release 16.1.1 よりも前のリリースで導入されました。

使用上のガイドライン

セッション番号が存在しないか、SPAN セッションがリモート接続先セッションの場合、コマンド出力には「% Error: No Information Available」のメッセージが表示されます。

次に、**show platform software swspan FP active source** コマンドの出力例を示します。

```
Switch# show platform software swspan FP active source sess-id 0

Showing SPAN source detail info

Session ID : 0
Intf Type : PORT
Port dpidx : 30
PD Sess ID : 1
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
AOM Object Status : Done
Parent AOM object Id : 118
Parent AOM object Status : Done

Session ID : 9
Intf Type : PORT
Port dpidx : 8
PD Sess ID : 0
Session Type : Local
Direction : Ingress
```

```
Filter Enabled : No
ACL Configured : No
AOM Object id : 578
AOM Object Status : Done
Parent AOM object Id : 70
Parent AOM object Status : Done
```

次に、**show platform software swspan RP active destination** コマンドの出力例を示します。

```
Switch# show platform software swspan RP active destination

Showing SPAN destination table summary info

Sess-id IF-type IF-id Sess-type
--------------------------------------
1 PORT 19 Remote
```

snmp-server enable traps

デバイスでネットワーク管理システム（NMS）にインフォーム要求やさまざまなトラップのSimple Network Management Protocol（SNMP）通知を送信可能にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps [**auth-framework** [**sec-violation**] | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]

no snmp-server enable traps [**auth-framework** [**sec-violation**] | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]

構文の説明

auth-framework	（任意）SNMP CISCO-AUTH-FRAMEWORK-MIB トラップをイネーブルにします。
sec-violation	（任意）SNMP camSecurityViolationNotif 通知をイネーブルにします。
bridge	（任意）SNMP STP ブリッジ MIB トラップをイネーブルにします。*
call-home	（任意）SNMP CISCO-CALLHOME-MIB トラップをイネーブルにします。*
cluster	（任意）SNMP クラスタ トラップをイネーブルにします。

config	（任意）SNMP 設定トラップをイネーブルにします。
config-copy	（任意）SNMP設定コピートラップをイネーブルにします。
config-ctid	（任意）SNMP 設定 CTID トラップをイネーブルにします。
copy-config	（任意）SNMP コピー設定トラップをイネーブルにします。
cpu	（任意）CPU 通知トラップをイネーブルにします。*
dot1x	（任意）SNMP dot1x トラップをイネーブルにします。*
energywise	（任意）SNMP energywise トラップをイネーブルにします。*
entity	（任意）SNMP エンティティ トラップをイネーブルにします。
envmon	（任意）SNMP環境モニタ トラップをイネーブルにします。*
errdisable	（任意）SNMPエラーディセーブル トラップをイネーブルにします。*
event-manager	（任意）SNMP 組み込みイベント マネージャ トラップをイネーブルにします。
flash	（任意）SNMP フラッシュ通知トラップをイネーブルにします。*
fru-ctrl	（任意）エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。デバイススタックでは、このトラップはスタックにおけるデバイスの挿入/取り外しを意味します。
license	（任意）ライセンス トラップをイネーブルにします。*
mac-notification	（任意）SNMP MAC 通知トラップをイネーブルにします。*
port-security	（任意）SNMPポートセキュリティ トラップをイネーブルにします。*
power-ethernet	（任意）SNMPパワーイーサネット トラップをイネーブルにします。*
rep	（任意）SNMP レジリエントイーサネットプロトコル トラップをイネーブルにします。
snmp	（任意）SNMP トラップをイネーブルにします。*

stackwise	（任意）SNMP StackWise トラップをイネーブルにします。*
storm-control	（任意）SNMP ストーム制御トラップ パラメータをイネーブルにします。
stpx	（任意）SNMP STPX MIB トラップをイネーブルにします。*
syslog	（任意）SNMP syslog トラップをイネーブルにします。
transceiver	（任意）SNMP トランシーバ トラップをイネーブルにします。*
tty	（任意）TCP 接続トラップを送信します。この設定はデフォルトでイネーブルになっています。
vlan-membership	（任意）SNMP VLAN メンバーシップ トラップをイネーブルにします。
vlancreate	（任意）SNMP VLAN 作成トラップをイネーブルにします。
vlandelete	（任意）SNMP VLAN 削除トラップをイネーブルにします。
vstack	（任意）SNMP スマートインストール トラップをイネーブルにします。*
vtp	（任意）VLAN トランキング プロトコル（VTP）トラップをイネーブルにします。

コマンド デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

上記の表のアスタリスクが付いているコマンドオプションにはサブ コマンドがあります。これらのサブ コマンドの詳細については、関連コマンドの項を参照してください。

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

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するには、**snmp-server enable traps** コマンドを使用します。

（注） コマンドラインのヘルプ ストリングに表示される場合でも、**fru-ctrl**、**insertion** および **removal** キーワードはデバイスでサポートされません。**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て使用します。

（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。

次に、複数の SNMP トラップ タイプをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps cluster
Device(config)# snmp-server enable traps config
Device(config)# snmp-server enable traps vtp
```

関連トピック

snmp-server enable traps bridge, （798 ページ）

snmp-server enable traps bulkstat, （799 ページ）

snmp-server enable traps call-home, （800 ページ）

snmp-server enable traps cef, （801 ページ）

snmp-server enable traps cpu, （802 ページ）

snmp-server enable traps envmon, （803 ページ）

snmp-server enable traps errdisable, （804 ページ）

snmp-server enable traps flash, （805 ページ）

snmp-server enable traps isis, （806 ページ）

snmp-server enable traps license, （807 ページ）
snmp-server enable traps mac-notification, （808 ページ）
snmp-server enable traps ospf, （809 ページ）
snmp-server enable traps pim, （811 ページ）
snmp-server enable traps port-security, （812 ページ）
snmp-server enable traps power-ethernet, （813 ページ）
snmp-server enable traps snmp, （814 ページ）
snmp-server enable traps stackwise, （815 ページ）
snmp-server enable traps storm-control, （818 ページ）
snmp-server enable traps stpx, （819 ページ）
snmp-server enable traps transceiver, （820 ページ）
snmp-server enable traps vrfmib, （821 ページ）
snmp-server enable traps vstack, （822 ページ）
snmp-server host, （824 ページ）

snmp-server enable traps bridge

STP ブリッジ MIB トラップを生成するには、グローバル コンフィギュレーション モードで **snmp-server enable traps bridge** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps bridge [**newroot**] [**topologychange**]

no snmp-server enable traps bridge [**newroot**] [**topologychange**]

構文の説明

newroot	（任意）SNMP STP ブリッジ MIB 新規ルート トラップをイネーブルにします。
topologychange	（任意）SNMP STP ブリッジ MIB トポロジ変更トラップをイネーブルにします。

コマンド デフォルト

ブリッジ SNMP トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次の例では、NMS にブリッジ新規ルート トラップを送信する方法を示します。

```
Device(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

データ収集 MIB トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps bulkstat** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps bulkstat [**collection** | **transfer**]

no snmp-server enable traps bulkstat [**collection** | **transfer**]

構文の説明

collection	（任意）データ収集 MIB 収集トラップをイネーブルにします。
transfer	（任意）データ収集 MIB 送信トラップをイネーブルにします。

コマンド デフォルト

データ収集 MIB トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、データ収集 MIB 収集トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

SNMP CISCO-CALLHOME-MIB トラップ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 **snmp-server enable traps call-home** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

no snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

構文の説明

message-send-fail	（任意）SNMP メッセージ送信失敗トラップをイネーブルにします。
server-fail	（任意）SNMP サーバ障害トラップをイネーブルにします。

コマンド デフォルト

SNMP CISCO-CALLHOME-MIB トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、SNMP メッセージ送信失敗トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

SNMP Cisco Express Forwarding（CEF）トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps cef** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

no snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

構文の説明

inconsistency	（任意）SNMP CEF 矛盾トラップをイネーブルにします。
peer-fib-state-change	（任意）SNMP CEF ピア FIB ステート変更トラップをイネーブルにします。
peer-state-change	（任意）SNMP CEF ピア ステート変更トラップをイネーブルにします。
resource-failure	（任意）SNMP リソース障害トラップをイネーブルにします。

コマンド デフォルト

SNMP CEF トラップの送信はディセーブルになります。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、SNMP CEF 矛盾トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps cpu

CPU 通知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 **snmp-server enable traps cpu** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps cpu [**threshold**]

no snmp-server enable traps cpu [**threshold**]

構文の説明

threshold	（任意）CPU しきい値通知をイネーブルにします。

コマンド デフォルト

CPU 通知の送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、CPU しきい値通知を生成する例を示します。

```
Device(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

SNMP 環境トラップ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 **snmp-server enable traps envmon** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps envmon [**fan**][**shutdown**][**status**] [**supply**][**temperature**]

no snmp-server enable traps envmon [**fan**][**shutdown**][**status**] [**supply**][**temperature**]

構文の説明

fan	（任意）ファン トラップをイネーブルにします。
shutdown	（任意）環境シャットダウン モニタ トラップをイネーブルにします。
status	（任意）SNMP 環境ステータス変更トラップをイネーブルにします。
supply	（任意）環境電源モニタ トラップをイネーブルにします。
temperature	（任意）環境温度モニタ トラップをイネーブルにします。

コマンド デフォルト

環境 SNMP トラップの送信はディセーブルになります。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、ファン トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps envmon fan
```

snmp-server enable traps errdisable

エラー ディセーブルの SNMP 通知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 **snmp-server enable traps errdisable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

構文の説明

notification-rate *number-of-notifications*	（任意）通知レートとして 1 分当たりの通知の数を指定します。受け入れられる値の範囲は 0 ～ 10000 です。

コマンド デフォルト

エラー ディセーブルの SNMP 通知送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、エラー ディセーブルの SNMP 通知数を 2 に設定する例を示します。

```
Device(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

SNMP フラッシュ通知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 **snmp-server enable traps flash** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps flash [**insertion**][**removal**]

no snmp-server enable traps flash [**insertion**][**removal**]

構文の説明

insertion	（任意）SNMP フラッシュ挿入通知をイネーブルにします。
removal	（任意）SNMP フラッシュ取り出し通知をイネーブルにします。

コマンド デフォルト

SNMP フラッシュ通知の送信はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、SNMP フラッシュ挿入通知を生成する例を示します。

```
Device(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps isis

Intermediate System-to-Intermediate System（IS-IS）リンクステート ルーティング プロトコル トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps isis** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps isis [**errors** | **state-change**]

no snmp-server enable traps isis [**errors** | **state-change**]

構文の説明

errors	（任意）IS-IS エラー トラップをイネーブルにします。
state-change	（任意）IS-IS ステート変更トラップをイネーブルにします。

コマンド デフォルト

IS-IS のトラップ送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、IS-IS エラー トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps isis errors
```

snmp-server enable traps license

ライセンス トラップ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 **snmp-server enable traps license** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps license [**deploy**][**error**][**usage**]

no snmp-server enable traps license [**deploy**][**error**][**usage**]

構文の説明

deploy	（任意）ライセンス導入トラップをイネーブルにします。
error	（任意）ライセンス エラー トラップをイネーブルにします。
usage	（任意）ライセンス使用トラップをイネーブルにします。

コマンド デフォルト

ライセンス トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、ライセンス導入トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

SNMP MAC 通知トラップ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 **snmp-server enable traps mac-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。

snmp-server enable traps mac-notification [**change**][**move**][**threshold**]

no snmp-server enable traps mac-notification [**change**][**move**][**threshold**]

構文の説明

change	（任意）SNMP MAC 変更トラップをイネーブルにします。
move	（任意）SNMP MAC 移動トラップをイネーブルにします。
threshold	（任意）SNMP MAC しきい値トラップをイネーブルにします。

コマンド デフォルト

SNMP MAC 通知トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、SNMP MAC 通知変更トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps ospf

SNMP の Open Shortest Path First（OSPF）トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps ospf** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]

no snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]

構文の説明

cisco-specific	（任意）シスコ固有のトラップをイネーブルにします。
errors	（任意）エラー トラップをイネーブルにします。
lsa	（任意）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。
rate-limit	（任意）レート制限トラップをイネーブルにします。

rate-limit-time	（任意）レート制限トラップの時間の長さを秒数で指定します。指定できる値は 2 ～ 60 です。
max-number-of-traps	（任意）設定した時間内に送信するレート制限トラップの最大数を指定します。
retransmit	（任意）パケット再送信トラップをイネーブルにします。
state-change	（任意）状態変更トラップをイネーブルにします。

コマンド デフォルト

OSPF SNMP トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、LSA トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps ospf lsa
```

snmp-server enable traps pim

SNMP Protocol-Independent Multicast（PIM）トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps pim** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps pim [**invalid-pim-message**][**neighbor-change**][**rp-mapping-change**]

no snmp-server enable traps pim [**invalid-pim-message**][**neighbor-change**][**rp-mapping-change**]

構文の説明

invalid-pim-message	（任意）無効な PIM メッセージ トラップをイネーブルにします。
neighbor-change	（任意）PIM ネイバー変更トラップをイネーブルにします。
rp-mapping-change	（任意）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。

コマンド デフォルト

PIM SNMP トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、無効な PIM メッセージ トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps port-security

SNMP ポート セキュリティ トラップ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 **snmp-server enable traps port-security** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps port-security [**trap-rate** *value*]

no snmp-server enable traps port-security [**trap-rate** *value*]

構文の説明

trap-rate*value*	（任意）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）。

コマンド デフォルト

ポート セキュリティ SNMP トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、1 秒当たり 200 の速度でポート セキュリティ トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps power-ethernet

SNMP の Power over Ethernet（PoE）トラップ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 **snmp-server enable traps power-ethernet** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps power-ethernet {**group** *number* | **police**}

no snmp-server enable traps power-ethernet {**group** *number* | **police**}

構文の説明

group*number*	指定したグループ番号に対するインライン パワー グループベース トラップをイネーブルにします。受け入れられる値の範囲は 1 ～ 9 です。
police	インライン パワー ポリシング トラップをイネーブルにします。

コマンド デフォルト

Power over Ethernet の SNMP トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、グループ 1 の Power over Ethernet（PoE）トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps poower-over-ethernet group 1
```

snmp-server enable traps snmp

SNMP トラップ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 **snmp-server enable traps snmp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps snmp [**authentication**][**coldstart**][**linkdown**] [**linkup**][**warmstart**]

no snmp-server enable traps snmp [**authentication**][**coldstart**][**linkdown**] [**linkup**][**warmstart**]

構文の説明

認証	（任意）認証トラップをイネーブルにします。
coldstart	（任意）コールド スタート トラップをイネーブルにします。
linkdown	（任意）リンクダウン トラップをイネーブルにします。
linkup	（任意）リンクアップ トラップをイネーブルにします。
warmstart	（任意）ウォーム スタート トラップをイネーブルにします。

コマンド デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、ウォーム スタートの SNMP トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps stackwise

SNMP StackWise トラップ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 **snmp-server enable traps stackwise** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps stackwise [**GLS**][**ILS**][**SRLS**] [**insufficient-power**][**invalid-input-current**] [**invalid-output-current**][**member-removed**][**member-upgrade-notification**] [**new-master**][**new-member**] [**port-change**][**power-budget-warning**][**power-invalid-topology**] [**power-link-status-changed**][**power-oper-status-changed**] [**power-priority-conflict**][**power-version-mismatch**][**ring-redundant**] [**stack-mismatch**][**unbalanced-power-supplies**][**under-budget**][**under-voltage**]

no snmp-server enable traps stackwise [**GLS**][**ILS**][**SRLS**] [**insufficient-power**][**invalid-input-current**] [**invalid-output-current**][**member-removed**][**member-upgrade-notification**] [**new-master**][**new-member**] [**port-change**][**power-budget-warning**][**power-invalid-topology**] [**power-link-status-changed**][**power-oper-status-changed**] [**power-priority-conflict**][**power-version-mismatch**][**ring-redundant**] [**stack-mismatch**][**unbalanced-power-supplies**][**under-budget**][**under-voltage**]

構文の説明

GLS	（任意）StackWise スタック電源 GLS トラップをイネーブルにします。

ILS	（任意）StackWise スタック電源 ILS トラップをイネーブルにします。
SRLS	（任意）StackWise スタック電源 SRLS トラップをイネーブルにします。
insufficient-power	（任意）Stackwise スタック電源の不平衡電源トラップをイネーブルにします。
invalid-input-current	（任意）Stackwise スタック電源の無効入力電流トラップをイネーブルにします。
invalid-output-current	（任意）Stackwise スタック電源の無効出力電流トラップをイネーブルにします。
member-removed	（任意）StackWise スタック メンバ削除トラップをイネーブルにします。
member-upgrade-notification	（任意）StackWise メンバのアップグレード用リロード トラップをイネーブルにします。
new-master	（任意）StackWise の新規マスター トラップをイネーブルにします。
new-member	（任意）StackWise の新規メンバ トラップをイネーブルにします。
port-change	（任意）StackWise のスタック ポート変更トラップをイネーブルにします。
power-budget-warning	（任意）StackWise スタック電源バジェット警告トラップをイネーブルにします。
power-invalid-topology	（任意）Stackwise スタック電源の無効トポロジ トラップをイネーブルにします。
power-link-status-changed	（任意）StackWise スタック電源リンク ステータス変更トラップをイネーブルにします。
power-oper-status-changed	（任意）StackWise スタック電源ポート動作ステータス変更トラップをイネーブルにします。
power-priority-conflict	（任意）StackWise スタック電源のプライオリティ競合トラップをイネーブルにします。
power-version-mismatch	（任意）StackWise スタック電源のバージョン不一致トラップをイネーブルにします。

ring-redundant	（任意）StackWiseのリング冗長トラップをイネーブルにします。
stack-mismatch	（任意）StackWise スタック不一致トラップをイネーブルにします。
unbalanced-power-supplies	（任意）Stackwiseスタック電源の不平衡電源トラップをイネーブルにします。
under-budget	（任意）StackWise スタック電源の不足バジェット トラップをイネーブルにします。
under-voltage	（任意）Stackwiseスタック電源の不足電圧トラップをイネーブルにします。

コマンド デフォルト

SNMP StackWise トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、StackWise スタック電源の GLS トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps stackwise GLS
```

snmp-server enable traps storm-control

SNMP ストーム制御トラップ パラメータ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 **snmp-server enable traps storm-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。

snmp-server enable traps storm-control {**trap-rate** *number-of-minutes*}

no snmp-server enable traps storm-control {**trap-rate**}

構文の説明

trap-rate *number-of-minutes*	（任意）SNMP ストーム制御トラップ レートを分単位で指定します。受け入れられる値の範囲は 0 ～ 1000 です。

コマンド デフォルト

SNMP ストーム制御トラップ パラメータの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、SNMP ストーム制御トラップレートを 1 分あたり 10 トラップに設定する例を示します。

```
Device(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

SNMP STPX MIB トラップ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 **snmp-server enable traps stpx** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps stpx [**inconsistency**][**loop-inconsistency**][**root-inconsistency**]

no snmp-server enable traps stpx [**inconsistency**][**loop-inconsistency**][**root-inconsistency**]

構文の説明

inconsistency	（任意）SNMP STPX MIB 矛盾更新トラップをイネーブルにします。
loop-inconsistency	（任意）SNMP STPX MIB ループ矛盾更新トラップをイネーブルにします。
root-inconsistency	（任意）SNMP STPX MIB ルート矛盾更新トラップをイネーブルにします。

コマンド デフォルト

SNMP STPX MIB トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、SNMP STPX MIB 矛盾更新トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

SNMP トランシーバ トラップ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 **snmp-server enable traps transceiver** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps transceiver {**all**}

no snmp-server enable traps transceiver {**all**}

構文の説明

all	（任意）すべての SNMP トランシーバ トラップをイネーブルにします。

コマンド デフォルト

SNMP トランシーバ トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、すべての SNMP トランシーバ トラップを設定する例を示します。

```
Device(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

SNMP vrfmib トラップを許可するには、グローバル コンフィギュレーション モードで **snmp-server enable traps vrfmib** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

no snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

構文の説明

vnet-trunk-down	（任意）vrfmib trunk ダウン トラップをイネーブルにします。
vnet-trunk-up	（任意）vrfmib trunk アップ トラップをイネーブルにします。
vrf-down	（任意）vrfmib vrf ダウン トラップをイネーブルにします。
vrf-up	（任意）vrfmib vrf アップ トラップをイネーブルにします。

コマンド デフォルト

SNMP vrfmib トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

この例は、vrfmib trunk ダウン トラップを生成する方法を示しています。

```
Device(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps vstack

SNMP スマート インストール トラップ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 **snmp-server enable traps vstack** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps vstack [**addition**][**failure**][**lost**][**operation**]

no snmp-server enable traps vstack [**addition**][**failure**][**lost**][**operation**]

構文の説明

addition	（任意）クライアントによって追加されたトラップをイネーブルにします。
failure	（任意）ファイルのアップロードとダウンロード障害トラップをイネーブルにします。
lost	（任意）クライアントの損失トラップをイネーブルにします。
operation	（任意）動作モード変更トラップをイネーブルにします。

コマンド デフォルト

SNMP スマート インストール トラップの送信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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（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。

次に、SNMP スマート インストール クライアント追加トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps vstack addition
```

snmp-server engineID

SNMP のローカル コピーまたはリモート コピーに名前を設定するには、グローバル コンフィギュレーション モードで **snmp-serverengineID** コマンドを使用します。

snmp-server engineID {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}

構文の説明

local*engineid-string*	SNMP コピーの名前に 24 文字の ID 文字列を指定します。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。
remote*ip-address*	リモート SNMP コピーを指定します。SNMP のリモート コピーを含むデバイスの *ip-address* を指定します。
udp-port*port-number*	（任意）リモート デバイスのユーザ データグラム プロトコル（UDP）ポートを指定します。デフォルトは 162 です。

コマンド デフォルト

なしグローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

次の例では、ローカル エンジン ID 1234000000000000000000000 を設定します。

```
Device(config)# snmp-server engineID local 1234
```

snmp-server host

Simple Network Management Protocol（SNMP）通知操作の受信者（ホスト）を指定するには、デバイスで **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* } [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

no snmp-server host {*host-addr* } [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

構文の説明

host-addr	ホスト（ターゲットとなる受信側）の名前またはインターネットアドレスです。
vrf*vrf-instance*	（任意）仮想プライベート 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。
informs | **traps**	（任意）このホストに SNMP トラップまたは情報を送信します。
version 1 | **2c** | **3**	（任意）トラップの送信に使用する SNMP のバージョンを指定します。 **1**：SNMPv1。情報の場合は、このオプションを使用できません。 **2c**：SNMPv2C。 **3**：SNMPv3。認証キーワードの1つ（次の表の行を参照）が、バージョン3キーワードに従っている必要があります。

auth | **noauth** | **priv**	**auth**（任意）：Message Digest 5（MD5）および Secure Hash Algorithm（SHA）によるパケット認証をイネーブルにします。 **noauth**（デフォルト）：noAuthNoPriv セキュリティ レベル。**auth** | **noauth** | **priv** キーワードの選択が指定されていない場合、これがデフォルトとなります。 **priv**（任意）：データ暗号規格（DES）によるパケット暗号化をイネーブルにします（privacy とも呼ばれます）。
community-string	通知処理にともなって送信される、パスワードと類似したコミュニティ ストリングです。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** グローバル コンフィギュレーション コマンドを使用してから、**snmp-server host** コマンドを使用することを推奨します。 （注） コンテキスト情報を区切るには@記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。
notification-type	（任意）ホストに送信される通知のタイプです。タイプが指定されていない場合、すべての通知が送信されます。通知タイプには、次のキーワードの 1 つまたは複数を指定できます。 • **auth-framework**：SNMP CISCO-AUTH-FRAMEWORK-MIB トラップを送信します。 • **bridge**：SNMP スパニングツリー プロトコル（STP）ブリッジ MIB トラップを送信します。 • **bulkstat**：データ収集 MIB 収集通知トラップを送信します。 • **call-home**：SNMP CISCO-CALLHOME-MIB トラップを送信します。 • **cef**：SNMP CEF トラップを送信します。 • **config**：SNMP 設定トラップを送信します。 • **config-copy**：SNMP 設定コピー トラップを送信します。 • **config-ctid**：SNMP 設定 CTID トラップを送信します。 • **copy-config**：SNMP コピー設定トラップを送信します。 • **cpu**：CPU 通知トラップを送信します。 • **cpu threshold**：CPU しきい値通知トラップを送信します。 • **eigrp**：SNMP EIGRP トラップを送信します。 • **entity**：SNMP エンティティ トラップを送信します。

- **envmon**：環境モニタ トラップを送信します。
- **errdisable**：SNMP エラー ディセーブル通知トラップを送信します。
- **event-manager**：SNMP Embedded Event Manager トラップを送信します。
- **flash**：SNMP フラッシュ通知を送信します。
- **flowmon**：SNMP フロー モニタ通知トラップを送信します。
- **ipmulticast**：SNMP IP マルチキャスト ルーティング トラップを送信します。
- **ipsla**：SNMP IP SLA トラップを送信します。
- **isis**：IS-IS トラップを送信します。
- **license**：ライセンス トラップを送信します。
- **local-auth**：SNMP ローカル認証トラップを送信します。
- **mac-notification**：SNMP MAC 通知トラップを送信します。
- **ospf**：Open Shortest Path First（OSPF）トラップを送信します。
- **pim**：SNMP Protocol-Independent Multicast（PIM）トラップを送信します。
- **port-security**：SNMP ポートセキュリティ トラップを送信します。
- **power-ethernet**：SNMP パワー イーサネット トラップを送信します。
- **snmp**：SNMP タイプ トラップを送信します。
- **storm-control**：SNMP ストーム制御トラップを送信します。
- **stpx**：SNMP STP 拡張 MIB トラップを送信します。
- **syslog**：SNMP syslog トラップを送信します。
- **transceiver**：SNMP トランシーバ トラップを送信します。
- **tty**：TCP 接続トラップを送信します。
- **vlan-membership**：SNMP VLAN メンバーシップ トラップを送信します。
- **vlancreate**：SNMP VLAN 作成トラップを送信します。
- **vlandelete**：SNMP VLAN 削除トラップを送信します。
- **vrfmib**：SNMP vrfmib トラップを送信します。
- **vstack**：SNMP スマート インストール トラップを送信します。
- **vtp**：SNMP VLAN Trunking Protocol（VTP）トラップを送信します。
- **wireless**：ワイヤレス トラップを送信します。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。通知は送信されません。

キーワードを指定しないでこのコマンドを入力した場合は、デフォルトで、すべてのトラップ タイプがホストに送信されます。情報はこのホストに送信されません。

version キーワードがない場合、デフォルトはバージョン 1 になります。

バージョン 3 を選択し、認証キーワードを入力しなかった場合は、デフォルトで、**noauth**（noAuthNoPriv）セキュリティ レベルになります。

（注） **fru-ctrl** キーワードは、コマンドラインのヘルプ ストリングには表示されていますが、サポートされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

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い場合、インフォーム要求を再送信して、インフォームが目的の宛先に到達する可能性を向上できます。

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。送信と同時に廃棄されるトラップと異なり、インフォーム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。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。

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デバイスを設定するには、**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 ホストと対応させられていない場合、デバイスは **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** コマンドを入力してから、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。

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。

```
Device(config)# snmp-server community comaccess ro 10
Device(config)# snmp-server host 172.20.2.160 comaccess
Device(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。

```
Device(config)# snmp-server enable traps
Device(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 に送信するようにデバイスをイネーブルにする方法を示します。

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

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

関連トピック

snmp-server enable traps

source（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元インターフェイスまたは VLAN、およびモニタするトラフィックの方向を設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **source** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

構文の説明

source {**interface***typenumber* | **vlan***vlan-ID*[,|-] [**both** | **rx** | **tx**]

interface*typenumber*	インターフェイスのタイプおよび番号を指定します。

vlan*vlan-ID*	ERSPAN 送信元セッション番号と VLAN を関連付けます。有効な値は 1 ～ 4094 です。
,	（任意）別のインターフェイスを指定します。
-	（任意）インターフェイスの範囲を指定します。
both	（任意）ERSPAN の送受信トラフィックをモニタします。
rx	（任意）受信トラフィックのみモニタします。
tx	（任意）送信トラフィックのみモニタします。

コマンド デフォルト

送信元インターフェイスまたは VLAN が設定されていません。

コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 VLAN とフィルタ VLAN を同じセッションに含めることはできません。

次に、ERSPAN 送信元セッションのプロパティの設定例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# source interface fastethernet 0/1 rx
```

関連コマンド

コマンド	説明
monitor session type erspan-source	ローカルの ERSPAN 送信元セッションを設定します。

switchport mode access

トランキングなし、タグなしの単一VLANイーサネットインターフェイスとしてインターフェイスを設定するには、テンプレート コンフィギュレーション モードで **switchport mode access** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport mode access

no switchport mode access

構文の説明

switchport mode access	トランキングなし、タグなしの単一 VLAN イーサネット インターフェイスとして、インターフェイスを設定します。

コマンド デフォルト

アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。アクセス ポートは、デフォルトで、VLAN 1 のトラフィックを送受信します。

コマンド モード

テンプレート 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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、単一 VLAN インターフェイスを設定する例を示します。

```
Device(config-template)# switchport mode access
```

switchport voice vlan

指定された VLAN からのすべての音声トラフィックを転送するように指定するには、テンプレート コンフィギュレーション モードで **switchport voice 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。

switchport voice vlan*vlan_id*

no switchport voice vlan

構文の説明

switchport voice vlan*vlan_id*	すべての音声トラフィックを指定された VLAN 経由で転送するように指定します。

コマンド デフォルト

1 ～ 4094 の値を指定できます。

コマンド モード

テンプレート 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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、指定された VLAN からのすべての音声トラフィックを転送するように指定する例を示します。

```
Device(config-template)# switchport voice vlan 20
```

第 XIV 部

QoS

- QoS コマンド，835 ページ

第 15 章

QoS コマンド

この章では、次の QoS コマンドについて説明します。

- auto qos classify, 836 ページ
- auto qos trust, 842 ページ
- auto qos video, 849 ページ
- auto qos voip, 859 ページ
- debug auto qos, 872 ページ
- show auto qos , 873 ページ
- class, 874 ページ
- class-map, 877 ページ
- match（クラスマップ コンフィギュレーション）, 879 ページ
- match non-client-nrt, 882 ページ
- match wlan user-priority, 883 ページ
- policy-map, 883 ページ
- priority, 886 ページ
- queue-buffers ratio, 888 ページ
- queue-limit, 890 ページ
- service-policy（有線）, 891 ページ
- service-policy（WLAN）, 893 ページ
- セット, 894 ページ
- show ap name service-policy, 902 ページ
- show ap name dot11, 903 ページ

- show class-map, 905 ページ
- show platform hardware fed switch, 906 ページ
- show platform software fed switch qos, 910 ページ
- show platform software fed switch qos qsb, 912 ページ
- show wireless client calls, 914 ページ
- show wireless client dot11, 915 ページ
- show wireless client mac-address（コール制御）, 916 ページ
- show wireless client mac-address（TCLAS）, 917 ページ
- show wireless client voice diagnostics, 918 ページ
- show policy-map, 919 ページ
- show wlan, 921 ページ
- trust device, 923 ページ

auto qos classify

QoS ドメイン内で信頼できないデバイスの Quality of Service（QoS）の分類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 classify** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos classify [police]

no auto qos classify [police]

構文の説明

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

コマンド デフォルト

auto-QoS 分類は、すべてのポートでディセーブルです。

コマンド モード

インターフェイス 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
Cisco IOS XE 3.2SE	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 ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、デバイス、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 デバイスなどが含まれます。

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

表 *32*：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	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

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

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

（注） デバイスは、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、デバイスをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

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

auto-QoS がイネーブルのときに自動的に生成される 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。

auto qos classify コマンドおよび **auto qos classify police** コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシーマップ（**auto qos classify police** コマンドの場合）：

- AutoQos-4.0-Classify-Police-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- AutoQos-4.0-Multimedia-Conf-Class（match-any）
- AutoQos-4.0-Bulk-Data-Class（match-any）
- AutoQos-4.0-Transaction-Class（match-any）
- AutoQos-4.0-Scavanger-Class（match-any）
- AutoQos-4.0-Signaling-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS を無効にするには、**no auto qos classify** インターフェイス コンフィギュレーション コマンドを使用します。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 を有効にした最後のポートで、**no auto qos classify** 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 は無効と見なされます（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）。

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

```
Device(config)# interface gigabitEthernet1/0/6
Device(config-if)# auto qos classify police
Device(config-if)# end
Device# show policy-map interface gigabitEthernet1/0/6

GigabitEthernet1/0/6

  Service-policy input: AutoQos-4.0-Classify-Police-Input-Policy

    Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af41
      police:
          cir 5000000 bps, bc 156250 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Bulk-Data
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af11
      police:
          cir 10000000 bps, bc 312500 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Transaction-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Transactional-Data
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af21
      police:
          cir 10000000 bps, bc 312500 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Scavanger-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Scavanger
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs1
      police:
          cir 10000000 bps, bc 312500 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
```

```
  Class-map: AutoQos-4.0-Signaling-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Signaling
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp cs3
    police:
        cir 32000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default
    police:
        cir 10000000 bps, bc 312500 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
```

```
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10
```

```
    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 25%
      queue-buffers ratio 25
```

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。

auto qos trust

QoS ドメイン内の信頼インターフェイスのサービス品質（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 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。

auto qos trust{**cos**| **dscp**}

no auto qos trust{**cos**| **dscp**}

構文の説明

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

コマンド デフォルト

auto-QoS 信頼は、すべてのポートでディセーブルです。

コマンド モード

インターフェイス 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
Cisco IOS XE 3.2SE	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 ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、デバイス、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 デバイスなどが含まれます。auto-QoS がイネーブルの場合は、入力パケットのラベル

を使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

表 *33*：トラフィック タイプ、パケット ラベル、およびキュー

	VoIP データ トラフィック	**VOIP** コントロール トラフィック	ルーティング プロトコル トラフィック	**STP**[5] **BPDU**[6] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[7]	46	24、26	48	56	34	–	
CoS[8]	5	3	6	7	3	–	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

5 STP = スパニング ツリー プロトコル
6 BPDU = ブリッジ プロトコル データ ユニット
7 DSCP = Differentiated Services Code Point（Diffserv コード ポイント）
8 CoS = Class of Service（サービス クラス）

表 *34*：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	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

（注） デバイスは、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、デバイスをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

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

auto-QoS がイネーブルのときに自動的に生成される 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。

auto qos trust cos コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos trust dscp コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy

- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS をディセーブルにするには、**no auto qos trust** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos trust** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

次に、特定の CoS 分類を持つ信頼できるインターフェイスの auto-QoS を有効にする方法を示します。

```
Device(config)# interface gigabitEthernet1/0/17
Device(config-if)# auto qos trust cos
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/17

GigabitEthernet1/0/17

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
```

```
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
```

```
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、特定の DSCP 分類を持つ信頼できるインターフェイスの auto-QoS を有効にする方法を示します。

```
Device(config)# interface GigabitEthernet1/0/18
Device(config-if)# auto qos trust dscp
Device(config-if)# end
Device#show policy-map interface GigabitEthernet1/0/18

GigabitEthernet1/0/18

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
```

```
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
```

```
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

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。

auto qos video

QoS ドメイン内のビデオのサービス品質（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 video** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos video {**cts** | **ip-camera** | **media-player**}

no auto qos video {**cts** | **ip-camera** | **media-player**}

構文の説明

cts	Cisco TelePresence System に接続されるポートを指定し、自動的にビデオの QoS を設定します。
ip-camera	Cisco IP カメラに接続されるポートを指定し、自動的にビデオの QoS を設定します。
media-player	Cisco Digital Media Player に接続されるポートを指定し、自動的にビデオの QoS を設定します。

コマンド デフォルト

Auto-QoS ビデオはコンポート上でディセーブルに設定されています。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 ドメイン内のビデオ トラフィックに適切な QoS を設定するには、このコマンドを使用します。QoS ドメインには、デバイス、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 デバイスなどが含まれます。auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。詳細については、この項の最後にあるキュー テーブルを参照してください。

auto-QoS は、Cisco TelePresence システム、Cisco IP カメラ、または Cisco Digital Media Player へのビデオ接続用にデバイスを設定します。

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。

デバイスは、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、デバイスをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

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

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

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

auto qos video cts コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos video ip-camera コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos video media-player コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS をディセーブルにするには、**no auto qos video** インターフェイス 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 を有効にした最後のポートで、**no auto qos video** 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 は無効と見なされます（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）。

表 *35*：トラフィック タイプ、パケット ラベル、およびキュー

	VoIP データ トラフィック	VOIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP[9] BPDU[10] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[11]	46	24、26	48	56	34	–	
CoS[12]	5	3	6	7	3	–	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）	2、3、6、7（キュー 2）	2、3、6、7（キュー 2）	0（キュー 3）	2（キュー 3）	0、1（キュー 4）

9 STP = スパニング ツリー プロトコル
10 BPDU = ブリッジ プロトコル データ ユニット
11 DSCP = DiffServ コード ポイント
12 CoS = サービス クラス

表 *36* : 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	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

次に、**auto qos video cts** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Device(config)# interface gigabitEthernet1/0/12
Device(config-if)# auto qos video cts
Device(config-if)# end
Device# show policy-map interface gigabitEthernet1/0/12

GigabitEthernet1/0/12

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
```

```
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
```

```
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos video ip-camera** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
Device(config)# interface GigabitEthernet1/0/9
Device(config-if)# auto qos video ip-camera
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/9

GigabitEthernet1/0/9

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
```

```
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10
```

```
    Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
      0 packets
      Match:  dscp af31 (26) af32 (28) af33 (30)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%
      queue-buffers ratio 10

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 25%
      queue-buffers ratio 25
```

次に、**auto qos video media-player** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Device(config)# interface GigabitEthernet1/0/7
Device(config-if)# auto qos video media-player
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/7

GigabitEthernet1/0/7

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
```

```
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
```

```
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

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

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**}

構文の説明

cisco-phone	Cisco IP Phone に接続されるポートを指定し、自動的にビデオの VoIP 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ます。
cisco-softphone	Cisco SoftPhone が動作している装置に接続されるポートを指定し、自動的にビデオの VoIP を設定します。
trust	信頼できるデバイスに接続されるポートを指定し、自動的にビデオの VoIP 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、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。

コマンド デフォルト

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 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、デバイス、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 デバイスなどが含まれます。

Auto-QoS は、デバイスとルーテッド 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動作する装置に対してデバイスを設定します。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。

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） デバイスは、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、デバイスをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

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

Cisco IP Phone に接続されたネットワーク エッジのポートで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、デバイスにより信頼境界の機能が有効になります。デバイスは、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone の存在を検出します。Cisco IP Phone が検出されると、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼するように設定されます。また、デバイス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、デバイスは DSCP 値を 0 に変更します。Cisco IP Phone が存在しない場合、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼しないように設定されます。ポリシングがポリシーマップ分類と一致したトラフィックに適用された後で、デバイスが信頼境界の機能をイネーブルにします。

-
- Cisco SoftPhone が動作するデバイス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、デバイス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、デバイスは DSCP 値を 0 に変更します。
- 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 コマンドを入力すると、非ルーテッド ポートの場合は入力パケット内の CoS 値、ルーテッド ポートの場合は入力パケット内の DSCP 値がデバイスで信頼されます（前提条件は、トラフィックがすでに他のエッジ デバイスによって分類されていることです）。

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 ポートで Cisco IP Phone の自動 QoS を有効にすると、スタティック IP アドレスを IP Phone に割り当てます。

（注） Cisco SoftPhone が稼働するデバイスがデバイスまたはルーテッド ポートに接続されている場合、デバイスはポートごとに 1 つの Cisco SoftPhone アプリケーションだけをサポートします。

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

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

auto qos voip trust コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）

- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos voip cisco-softphone コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- AutoQos-4.0-Voip-Data-Class（match-any）
- AutoQos-4.0-Voip-Signal-Class（match-any）
- AutoQos-4.0-Multimedia-Conf-Class（match-any）
- AutoQos-4.0-Bulk-Data-Class（match-any）
- AutoQos-4.0-Transaction-Class（match-any）
- AutoQos-4.0-Scavanger-Class（match-any）
- AutoQos-4.0-Signaling-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos voip cisco-phone コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
- service-policy output AutoQos-4.0-Output-Policy

クラス マップ：

- class AutoQos-4.0-Voip-Data-CiscoPhone-Class
- class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
- class AutoQos-4.0-Default-Class

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）。

デバイスは、このテーブルの設定にしたがってポートの出力キューを設定します。

表 *37*：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	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

次に、**auto qos voip trust** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Device(config)# interface gigabitEthernet1/0/31
Device(config-if)# auto qos voip trust
Device(config-if)# end
Device# show policy-map interface GigabitEthernet1/0/31

GigabitEthernet1/0/31

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy
```

```
  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
    Match:  dscp af21 (18) af22 (20) af23 (22)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  2
      0 packets, 0 bytes
      5 minute rate 0 bps
```

```
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
    0 packets
    Match:  dscp af11 (10) af12 (12) af13 (14)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  1
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 4%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos voip cisco-phone** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Device(config)# interface gigabitEthernet1/0/5
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# end
Device# show policy-map interface gigabitEthernet1/0/5

GigabitEthernet1/0/5

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
```

```
    0 packets
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp ef
    police:
        cir 128000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
    0 packets
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp cs3
    police:
        cir 32000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
```

```
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
```

```
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos voip cisco-softphone** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Device(config)# interface gigabitEthernet1/0/20
Device(config-if)# auto qos voip cisco-softphone
Device(config-if)# end
Device# show policy-map interface gigabitEthernet1/0/20

 GigabitEthernet1/0/20

  Service-policy input: AutoQos-4.0-CiscoSoftPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
      0 packets
      Match:  dscp ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
      0 packets
      Match:  dscp cs3 (24)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs3
      police:
          cir 32000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
        0 packets, 0 bytes
```

```
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
      cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavanger
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Signaling
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
```

```
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default
    police:
        cir 10000000 bps, bc 312500 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
```

```
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
    Match:  dscp af21 (18) af22 (20) af23 (22)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  2
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
    0 packets
    Match:  dscp af11 (10) af12 (12) af13 (14)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  1
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 4%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

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。

debug auto qos

Automatic Quality of Service（auto-QoS; 自動 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

構文の説明

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-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
Cisco IOS XE 3.2SE	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-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。デバッグをイネーブルにするには、**debug auto qos** 特権 EXEC コマンドを入力します。

undebug auto qos コマンドは、**no debug auto qos** コマンドと同じです。

あるデバイス スタック上でデバッグをイネーブルにした場合、アクティブデバイスでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session***switch-number* 特権 EXEC コマンドでアクティブ デバイスからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ デバイスのデバッグをイネーブルにするには、アクティブ デバイス上で **remote command***stack-member-numberLINE* 特権 EXEC コマンドを使用します。

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。

```
Device# debug auto qos
```

```
AutoQoS debugging is on
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# auto qos voip cisco-phone
```

show auto qos

automatic QoS（auto-QoS）が有効になっているインターフェイスに入力された Quality of Service（QoS）コマンドを表示するには、特権 EXEC モードで **show auto qos** コマンドを使用します。

show auto qos [**interface** [*interface-id*]]

構文の説明

interface [*interface-id*]	（任意）指定されたポートまたはすべてのポートの auto-QoS 情報を表示します。有効なインターフェイスには、物理ポートが含まれます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

Cisco IOS リリース 12.2(40)SE 以降、**show auto qos** コマンドの出力には、Cisco IP Phone のサービス ポリシー情報が表示されます。

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。

```
Device# show auto qos
GigabitEthernet2/0/4
auto qos voip cisco-softphone

GigabitEthernet2/0/5
auto qos voip cisco-phone


GigabitEthernet2/0/6
auto qos voip cisco-phone
```

次の例では、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos interface***interface-id* コマンドの出力を示します。

```
Device# show auto qos interface gigabitethernet 2/0/5
GigabitEthernet2/0/5
auto qos voip cisco-phone
```

次の例では、**auto qos voip cisco-phone** 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。

```
Device# show auto qos interface gigabitethernet1/0/2
GigabitEthernet1/0/2
auto qos voip cisco-phone
```

次の例では、auto-QoS がインターフェイスでディセーブルになっている場合の **show auto qos interface***interface-id* コマンドの出力を示します。

```
Device# show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled
```

class

指定されたクラスマップ名のトラフィックを分類する一致基準を定義するには、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*| **class-default**}

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

構文の説明

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

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。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 モードが開始されます。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。

- **admit**：コール アドミッション制御（CAC）の要求を許可します。
- **bandwidth**：クラスに割り当てられる帯域幅を指定します。
- **exit**：ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
- **no**：コマンドをデフォルト設定に戻します。
- **police**：分類したトラフィックのポリサーまたは集約ポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。このコマンドの詳細については、『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。
- **priority**：ポリシーマップに属するトラフィックのクラスにスケジューリング プライオリティを割り当てます。
- **queue-buffers**：クラスのキュー バッファを設定します。
- **queue-limit**：ポリシー マップに設定されたクラス ポリシー用にキューが保持できる最大パケット数を指定します。
- **service-policy**：QoS サービス ポリシーを設定します。
- **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、次のサイトを参照してください。 セット，（894 ページ）
- **shape**：平均またはピーク レート トラフィック シェーピングを指定します。このコマンドの詳細については、『*Cisco IOS Quality of Service Solutions Command Reference*』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。

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

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

次に、policy1 という名前のポリシーマップを作成する例を示します。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。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した DSCP 値がマークされてから送信されます。

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

次に、ポリシー マップにデフォルトのトラフィック クラスを設定する例を示します。また、**class-default** が最初に設定された場合でも、デフォルトのトラフィック クラスをポリシー マップ pm3 の終わりに自動的に配置する方法も示します。

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

関連トピック

class-map, （877 ページ）
policy-map, （883 ページ）
show policy-map, （919 ページ）
セット, （894 ページ）

class-map

名前を指定したクラスとパケットの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーションモードを開始するには、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またはポリシー マップ コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

match-any	（任意）このクラス マップ内の一致ステートメントの論理和をとります。1 つ以上の条件が一致していなければなりません。
type	（任意）CPL クラス マップを設定します。
class-map-name	クラス マップ名。

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。

コマンド モード

グローバル コンフィギュレーション

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**type** キーワードが追加されました。

使用上のガイドライン

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

ポートごとに適用される、グローバルに名前が付けられたサービス ポリシーの一部として、パケットの分類、マーキング、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。
- **no**：クラス マップから一致ステートメントを削除します。

match-any キーワードを入力した場合、**match access-group** クラスマップ コンフィギュレーション コマンドで名前付き拡張アクセス コントロール リスト（ACL）を指定するためだけに使用できます。

物理ポート単位でパケット分類を定義するために、クラス マップごとに 1 つの **match** コマンドのみがサポートされています。

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。

次に、クラス マップ class1 に 1 つの一致基準（アクセス リスト 103）を設定する例を示します。

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

次に、クラス マップ class1 を削除する例を示します。

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

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

関連トピック

policy-map, （883 ページ）

show policy-map, （919 ページ）

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**{**name***acl-name* | *acl-index*}| **class-map** *class-map-name*| **cos** *cos-value*| **dscp** *dscp-value*| **[ip] dscp** *dscp-list* | **[ip] precedence** *ip-precedence-list*| **precedence** *precedence-value1...value4*| **qos-group** *qos-group-value*| **vlan** *vlan-id*}

no match {**access-group**{**name***acl-name* | *acl-index*}| **class-map** *class-map-name*| **cos** *cos-value*| **dscp** *dscp-value*| **[ip] dscp** *dscp-list* | **[ip] precedence** *ip-precedence-list*| **precedence** *precedence-value1...value4*| **qos-group** *qos-group-value*| **vlan** *vlan-id*}

構文の説明

access-group	アクセス グループを指定します。
name *acl-name*	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 の名前を指定します。
acl-index	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。
class-map *class-map-name*	トラフィック クラスを分類ポリシーとして使用し、使用するトラフィック クラスの名前を一致基準として指定します。
cos *cos-value*	レイヤ 2 サービス クラス（CoS）/Inter-Switch Link（ISL）マーキングに基づいてパケットを照合します。CoS 値は 0 ～ 7 です。1 つの **match cos** ステートメントに最大 4 つの CoS 値をスペースで区切って指定できます。
dscp *dscp-value*	各 DSCP 値のパラメータを指定します。DiffServ コード ポイント値を指定する 0 ～ 63 の範囲の値を指定できます。
ip dscp*dscp-list*	着信パケットとの照合を行うための、最大 8 つまでの IP DiffServ コード ポイント（DSCP）値の一覧を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。一般的に使用する値に対してはニーモニック名を入力することもできます。

ip precedence*ip-precedence-list*	着信パケットとの照合を行うための、最大 8 つの IP プレシデンス値の一覧を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 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。
precedence *precedence-value1...value4*	分類されたトラフィックに IP プレシデンス値を割り当てます。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。
qos-group *qos-group-value*	特定の QoS グループ値を一致基準として識別します。指定できる範囲は 0 ～ 31 です。
vlan *vlan-id*	特定の VLAN を一致基準として指定します。指定できる範囲は 1 ～ 4095 です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**class-map** *class-map-name*、**cos** *cos-value*、**qos-group** *qos-group-value*、および **vlan** *vlan-id* キーワードが追加されました。

使用上のガイドライン

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。

class-map match-any*class-map-name* グローバル コンフィギュレーション コマンドを入力する場合、次の **match** コマンドを入力できます。

- **match access-group name** *acl-name*

（注） ACL は、名前付き拡張 ACL にする必要があります。

- **match ip dscp***dscp-list*
- **match ip precedence***ip-precedence-list*

match access-group*acl-index* コマンドはサポートされていません。

物理ポート単位でパケット分類を定義するために、クラス マップごとに 1 つの **match** コマンドのみがサポートされています。この場合、**match-any** キーワードと同じです。

match ip dscp*dscp-list* 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 ipprecedence 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一覧を表示するには、**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文字列を参照してください。

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。

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。

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(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。

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(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。

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(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。

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(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。

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

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

match non-client-nrt

NRT（非リアルタイム）で非クライアントを照合するには、クラスマップ コンフィギュレーション モードで **matchnon-client-nrt** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match non-client-nrt

no match non-client-nrt

構文の説明

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

クラスマップ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

次に、NRT で非クライアントを設定する例を示します。

```
Device(config)# class-map test_1000
Device(config-cmap)# match non-client-nrt
```

match wlan user-priority

802.11 固有の値を照合するには、クラスマップ コンフィギュレーション モードで **matchwlanuser-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。

match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

no match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

構文の説明

wlan-value	802.11 固有の値。ユーザ プライオリティ 802.11 TID user priority（0-7）を入力します。（任意）ユーザ プライオリティ値を 3 つまで、空白文字区切りで入力します。

コマンド デフォルト

なし

コマンド モード

クラスマップ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

次に、ユーザ プライオリティ値を設定する例を示します。

```
Device(config)# class-map test_1000
Device(config-cmap)# match wlan user-priority 7
```

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。
- **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。
- **sequence-interval**：シーケンス番号機能をイネーブルにします。

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。

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 に適用できます。

物理ポートに非階層ポリシーマップを適用できます。非階層ポリシーマップは、デバイスのポート ベース ポリシー マップと同じです。

階層ポリシー マップには親子ポリシーの形式で 2 つのレベルがあります。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。

VLAN ベースの QoS では、サービス ポリシーが SVI インターフェイスに適用されます。VLAN ポリシーマップに属するすべての物理インターフェイスは、ポートベースのポリシーマップの代わりに VLAN ベースのポリシー マップが表示されるように設定する必要があります。

（注） 有線およびワイヤレスポートですべての MQC QoS の組み合わせがサポートされているわけではありません。これらの制限の詳細については、サービス品質（QoS）構成ガイドの「有線ターゲットのQoSの制限」および「ワイヤレス ターゲットの QoS の制限」に関する章を参照してください。

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。プロファイル未満のトラフィックが送信されます。

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

次に、階層ポリシーを設定する例を示します。

```
Switch# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit
```

```
Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

次に、ポリシー マップを削除する例を示します。

```
Device(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。

関連トピック

class, （874 ページ）

class-map, （877 ページ）

service-policy（有線）, （891 ページ）

show policy-map, （919 ページ）

priority

ポリシー マップに属するトラフィックのクラスにプライオリティを割り当てるには、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 **priority** コマンドを使用します。以前に指定したクラスのプライオリティを削除するには、このコマンドの **no** 形式を使用します。

priority [*Kbps* [*burst -in-bytes*] | **level** *level-value* [*Kbps* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]

no priority [*Kb/s* [*burst -in-bytes*] | **level** *level value* [*Kb/s* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]

構文の説明

Kb/s	（任意）プライオリティ トラフィック向けの保証帯域幅（キロビット/秒（kbps））。帯域幅の量は、使用中のインターフェイスとプラットフォームによって異なります。保証帯域幅を超えると、非プライオリティ トラフィックがなくならないようにするため、プライオリティ トラフィックが輻輳のイベントでドロップされます。値は 1 ～ 2,000,000 kbps である必要があります。
burst -in-bytes	（任意）バイト単位のバースト サイズ。バースト サイズは、トラフィックの一時的なバーストに対応するネットワークを設定します。デフォルト バースト値は、設定されている帯域幅レートで、200 ミリ秒のトラフィックとして計算され、burst 引数が指定されていない場合に使用されます。バーストの範囲は 32 ～ 2000000 バイトです。

level*level-value*	（任意）プライオリティ レベルを割り当てます。*level-value* の有効値は 1 と 2 です。レベル 1 はレベル 2 よりもプライオリティが高くなります。レベル 1 は帯域幅を予約して最初に送信を行うため、遅延は非常に低くなります。使用しない場合でも、帯域幅を予約します。レベル 1 および 2 はどちらも帯域幅を予約できます。
percent*percentage*	（任意）保証帯域幅の量が、使用可能な帯域幅の割合（%）によって指定されることを、指定します。

コマンド デフォルト

プライオリティは設定されません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	*Kbps*、*burst -in-bytes* および **percent***percentage* キーワードが追加されました。

使用上のガイドライン

このコマンドは、クラスベース WFQ（CBWFQ）の完全プライオリティ キューイング（PQ）の場合に、低遅延キューイング（LLQ）を設定します。完全 PQ では、音声などの遅延に敏感なデータを、他のキューのパケットをキューから取り出す前にキューから取り出して送信できます。

（注） プライオリティは 1 つのレベルのみ設定できます。
1 つのポリシーマップで使用できる完全プライオリティまたはレベル付きプライオリティは 1 つだけです。kbps または割合のない同じプライオリティ レベルが設定された複数のプライオリティは、ポリシングですべてが設定された場合にのみ使用できます。

priority コマンドを使用すると、（User Datagram Ports（UDP）ポートだけではなく）さまざまな基準に基づいてクラスと設定し、プライオリティを割り当てることができます。これは、シリアル インターフェイスと ATM 相手先固定接続（PVC）で使用できます。類似の **ip rtp priority** コマン

ドを使用すると、UDPポート番号にだけ基づいてプライオリティフローを決定することができ、ATM PVC は使用できません。

デバイスが輻輳していない場合は、プライオリティクラストラフィックの割り当て帯域幅を超えることができます。デバイスが輻輳している場合、割り当てられた帯域幅を超えるプライオリティクラス トラフィックは破棄されます。

同じポリシー マップ内では、bandwidth コマンドおよび priority コマンドは、同じクラスに使用できません。ただし、これらのコマンドは、同じポリシー マップ内では一緒に使用できます。

ポリシー マップで、1 つまたは複数のクラスにプライオリティ ステータスを指定できます。単一ポリシーマップ内の複数のクラスがプライオリティクラスとして設定されると、これらのクラスからのすべてのトラフィックが、同じ単一のプライオリティ キューにキューイングされます。

クラスポリシー設定が含まれているポリシーマップがインターフェイスに付加されて、そのインターフェイスのサービス ポリシーが決定される場合、使用可能な帯域幅が評価されます。インターフェイスの帯域幅が不十分なことが原因で、特定のインターフェイスにポリシー マップがアタッチできない場合、そのポリシーは、正常にアタッチされていたすべてのインターフェイスから削除されます。

例

次に、ポリシー マップ policy1 のクラスのプライオリティを設定する例を示します。

```
Device(config)# class-map cm1
Device(config-cmap)#match precedence 2
Device(config-cmap)#exit

Device(config)#class-map cm2
Device(config-cmap)#match dscp 30
Device(config-cmap)#exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 1m
Device(config-pmap-c-police)#exit
Device(config-pmap-c)#exit
Device(config-pmap)#exit

Device(config)#policy-map policy1
Device(config-pmap)#class cm2
Device(config-pmap-c)#priority level 2
Device(config-pmap-c)#police 1m
```

queue-buffers ratio

クラスのキュー バッファを設定するには、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 **queue-buffers ratio** コマンドを使用します。比率制限を削除するには、このコマンドの **no** 形式を使用します。

queue-buffers ratio *ratio limit*

no queue-buffers ratio *ratio limit*

構文の説明

ratio limit	（任意）クラスのキューバッファを設定します。キューバッファの比率制限（0 ～ 100）を入力します。

コマンド デフォルト

クラスのキュー バッファ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
Cisco IOS XE 3.2SE	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前に、**bandwidth**、**shape** または **priority** コマンドを使用する必要があります。これらのコマンドの詳細については、Cisco.com で入手可能な *Cisco IOS Quality of Service* ソリューションのコマンド リファレンスを参照してください。

を使用すると、キューにバッファを割り当てることができます。バッファが割り当てられていない場合、すべてのキューの間で均等に分割されます。queue-buffer ratio を使用して、特定の比率で分割できます。デフォルトでは、ダイナミックしきい値およびスケーリング（DTS）がすべてのキューでアクティブであるため、バッファはソフト バッファです。

（注） queue-buffer ratio は有線ポートと無線ポートの両方でサポートされますが、queue-buffer ratio は queue-limit とともに設定することはできません。

例

次にキュー バッファの比率を 10 % に設定する例を示します。

```
Device(config)# policy-map policy_queuebuf01
Device(config-pmap)# class-map class_queuebuf01
Device(config-cmap)# exit
Device(config)# policy policy_queuebuf01
Device(config-pmap)# class class_queuebuf01
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# queue-buffers ratio 10
```

```
Device(config-pmap)# end
```

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

関連トピック

show policy-map, （919 ページ）

queue-limit

キューが保持できる、ポリシーマップ内に設定されたクラスポリシーのパケットの最大数を指定または変更するには、**queue-limit** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。クラスからキュー パケット制限を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *queue-limit-size*[**packets**] {**cos** *cos-value*| **dscp** *dscp-value*} **percent** *percentage-of-packets*

no queue-limit *queue-limit-size*[**packets**] {**cos** *cos-value*| **dscp** *dscp-value*} **percent** *percentage-of-packets*

構文の説明

queue-limit-size	キューの最大サイズ。最大値は、オプションの指定される測定単位用キーワード（bytes、ms、または packets）の単位によって異なります。
cos *cos-value*	各 cos 値のパラメータを指定します。CoS 値の範囲は 0 ～ 7 です。
dscp *dscp-value*	各 DSCP 値のパラメータを指定します。 キュー制限のタイプに合わせて DiffServ コードポイント値を指定します。範囲は 0 ～63 です。
percent *percentage-of-packets*	このクラスのキューが蓄積できるパケットの最大割合を指定します。範囲は 1 ～ 100 です。

コマンド デフォルト

なし

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

packets 測定単位は、コマンドラインのヘルプ文字列には表示されますが、サポートされていません。**percent** 測定単位を使用してください。

（注） このコマンドは、出力方向の有線ポートでのみサポートされています。

Weighted Fair Queueing（WFQ）により、クラス マップが定義される各クラスのキューが作成されます。クラスの一致条件を満たすパケットは、送信されるまで、このクラス専用のキューに蓄積されます。この処理は、均等化キューイング プロセスによってキューが処理される場合に発生します。クラスに定義した最大パケットしきい値に達すると、クラス キューへのそれ以降のパケットのキューイングは、テール ドロップされます。

重み付けテール ドロップ（WTD）を設定するためにキュー制限を使用します。WTD を使用すると、キューごとに複数のしきい値を設定できます。各サービス クラスが異なるしきい値でドロップされて QoS 差別化が実現されます。

トラフィックの異なるサブクラス、つまり、DSCP と CoS に最大キューしきい値を設定し、各サブクラスに最大キューしきい値を設定できます。

例

次の例では、dscp-1 というクラスのポリシーを含めるために port-queue というポリシー マップを設定しています。このクラスのポリシーは、確保されているキューの最大パケット制限が20％になるように設定されています。

```
Device(config)# policy-map policy11
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```

service-policy（有線）

物理ポートまたはスイッチ仮想インターフェイス（SVI）のにポリシー マップを適用するには、インターフェイス コンフィギュレーション モードで **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** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *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。
output*policy-map-name*	物理ポートまたは SVI の出力に、指定したポリシー マップを適用します。

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

WLAN インターフェイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

ポリシー マップは、**policy map** コマンドによって定義されます。

1 つのポートごとに入力と出力に関して 1 つのポリシーマップだけがサポートされます。つまり、いずれのポートにおいても、1 つの入力ポリシーと 1 つの出力ポリシーだけを使用できます。

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。*QoS Configuration Guide (Catalyst 3850 Switches)*。

（注） **history** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。このキーワードが収集した統計情報は無視します。

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。

```
Device(config)# interface gigabitethernet2/0/1
Device(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。

```
Device(config)# interface gigabitethernet2/0/2
Device(config-if)# no service-policy input plcmap2
```

次の例では、VLAN のポリサー設定を表示します。この設定の最後に、QoS のインターフェイスに VLAN ポリシー マップを適用します。

```
Device# configure terminal
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
Device(config)# interface gigabitEthernet1/0/5
Device(config-if)#  service-policy input vlan100
```

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。

関連トピック

policy-map, （883 ページ）

show policy-map, （919 ページ）

service-policy（WLAN）

WLAN サービス品質（QoS）サービス ポリシーを設定するには、**service-policy** コマンドを使用します。WLAN の QoS ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

service-policy [client] {**input| output**}*policy-name*

no service-policy [client] {**input| output**}*policy-name*

構文の説明

client	（任意）WLAN 上のすべてのクライアントにポリシー マップを割り当てます。
input	入力ポリシー マップを割り当てます。
output	出力ポリシー マップを割り当てます。
policy-name	ポリシー名。

コマンド デフォルト

ポリシーが割り当てられない場合、ポリシーに割り当てられる状態は [None] になります。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次の例では、WLAN の入力 QoS サービス ポリシーを設定する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy input policy-test
```

次の例では、WLAN の入力 QoS サービス ポリシーをディセーブルにする方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no service-policy input policy-test
```

次に、WLAN の出力 QoS サービス ポリシーを platinum（貴金属ポリシー）に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy output platinum
```

関連トピック

wlan, （1518 ページ）

wlan, （1518 ページ）

セット

パケットで Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値または IP プレシデンス値を設定して IP トラフィックを分類するには、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 **set** 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 cos| dscp| precedence| ip| qos-group| wlan

set cos {*cos-value*} | {**cos| dscp| precedence| qos-group| wlan**} [**table** *table-map-name*]

set dscp {*dscp-value*} | {**cos| dscp| precedence| qos-group| wlan**} [**table** *table-map-name*]

set ip{**dscp| precedence**}

set precedence{*precedence-value*} | {**cos| dscp| precedence| qos-group**} [**table** *table-map-name*]

set qos-group {*qos-group-value*| **dscp** [**table** *table-map-name*]| **precedence** [**table** *table-map-name*]}

set wlan user-priority*user-priority-value*| **costable** *table-map-name*| **dscptable** *table-map-name*| **qos-grouptable** *table-map-name*| **wlantable** *table-map-name*

構文の説明

cos	発信パケットのレイヤ 2 サービス クラス（CoS）値またはユーザ プライオリティを設定します。次の値を指定できます。 • *cos-value*：0 ～ 7 の CoS 値。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。 • パケットに CoS 値を設定するためのパケット マーキング カテゴリを指定します。パケット マーキング値をマッピングおよび変換するためのテーブルマップも設定している場合は、これによって「map from」パケットマーキング カテゴリが確立されます。パケットマーキング カテゴリのキーワードは次のとおりです。 ◦ **cos**：CoS 値またはユーザ プライオリティからの値を設定します。 ◦ **dscp**：DiffServ コード ポイント（DSCP）からの値を設定します。 ◦ **precedence**：パケット優先順位からの値を設定します。 ◦ **qos-group**：QoS グループからの値を設定します。 ◦ **wlan**：WLAN ユーザ プライオリティ値を設定します。 • （任意）**table** *table-map-name*：CoS 値の設定に使用される指定されたテーブルマップに設定されている値を示します。CoS 値の指定に使用されるテーブルマップの名前を入力します。テーブル マップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を CoS 値としてコピーすることです。たとえば、**set cos precedence** コマンドを入力する場合、precedence（パケット マーキング カテゴリ）値がコピーされ、CoS 値として使用されます。

dscp	IP（v4）および IPv6 パケットの DiffServ コード ポイント（DSCP）を指定します。次の値を指定できます。 • *cos-value*：DSCP 値を設定する番号。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。 • パケットに DSCP 値を設定するためのパケット マーキング カテゴリを指定します。パケット マーキング値をマッピングおよび変換するためのテーブルマップも設定している場合は、これによって「map from」パケットマーキング カテゴリが確立されます。パケットマーキング カテゴリのキーワードは次のとおりです。 ◦ **cos**：CoS 値またはユーザ プライオリティからの値を設定します。 ◦ **dscp**：DiffServ コード ポイント（DSCP）からの値を設定します。 ◦ **precedence**：パケット優先順位からの値を設定します。 ◦ **qos-group**：QoS グループからの値を設定します。 ◦ **wlan**：WLAN からの値を設定します。 • （任意）**table** *table-map-name*：DSCP 値の設定に使用される指定されたテーブルマップに設定されている値を示します。DSCP 値の指定に使用されるテーブルマップの名前を入力します。テーブル マップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を DSCP 値としてコピーすることです。たとえば、**set dscp cos** コマンドを入力する場合、CoS 値（パケットマーキング カテゴリ）がコピーされ、DSCP 値として使用されます。

ip	分類されたトラフィックにIP値を設定します。次の値を指定できます。 • **dscp**：0～63 の IP DSCP 値またはパケット マーキング カテゴリを指定します。 • **precedence**：IP ヘッダーの precedence ビット値を指定します（有効な値は0～7）。または、パケットマーキング カテゴリを指定します。
precedence	パケット ヘッダーに precedence 値を設定します。次の値を指定できます。 • *precedence-value*：パケット ヘッダーに precedence ビットを設定します。有効な値は 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。 • パケットの優先順位値を設定するためのパケットマーキング カテゴリを指定します。 ◦ **cos**：CoS またはユーザ プライオリティからの値を設定します。 ◦ **dscp**：DiffServ コード ポイント（DSCP）からの値を設定します。 ◦ **precedence**：パケット優先順位からの値を設定します。 ◦ **qos-group**：QoS グループからの値を設定します。 • （任意）**table** *table-map-name*：優先順位値の設定に使用される指定されたテーブルマップに設定されている値を示します。優先順位値の指定に使用されるテーブルマップの名前を入力します。テーブル マップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を優先順位値としてコピーすることです。たとえば、**set precedence cos** コマンドを入力する場合、CoS 値（パケットマーキング カテゴリ）がコピーされ、優先順位値として使用されます。

qos-group	後でパケットを分類するために使用できる QoS グループ ID を割り当てます。 • *qos-group-value*：分類されたトラフィックに QoS 値を設定します。指定できる範囲は 0 ～ 31 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。 • **dscp**：パケットの元の DSCP フィールド値を QoS グループ値として設定します。 • **precedence**：パケットの元の優先順位フィールドの値を QoS グループ値として設定します。 •（任意）**table** *table-map-name*：DSCP 値または優先順位値の設定に使用される指定されたテーブルマップに設定されている値を示します。値の指定に使用されるテーブルマップの名前を入力します。テーブル マップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリ（**dscp** または **precedence**）を指定したが、テーブルマップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を QoS グループ値としてコピーすることです。たとえば、**set qos-group precedence** コマンドを入力する場合、優先順位値（パケット マーキング カテゴリ）がコピーされ、QoS グループ値として使用されます。

wlanuser-priority*wlan-user-priority*	分類されたトラフィックに WLAN ユーザ プライオリティを割り当てます。次の値を指定できます。 • *wlan-user-priority*：分類されたトラフィックに WLAN ユーザ プライオリティを設定します。指定できる範囲は 0 ～ 7 です。 • **cos**：レイヤ 2 CoS フィールド値を WLAN ユーザ プライオリティとして設定します。 • **dscp**：DSCP フィールド値を WLAN ユーザ プライオリティとして設定します。 • **precedence**：優先順位フィールド値を WLAN ユーザ プライオリティとして設定します。 • **wlan**：WLAN ユーザ プライオリティ フィールド値を WLAN ユーザ プライオリティとして設定します。 • （任意）**table** *table-map-name*：WLAN ユーザ プライオリティ値の設定に使用される指定されたテーブルマップに設定されている値を示します。値の指定に使用されるテーブルマップの名前を入力します。テーブルマップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を WLAN ユーザ プライオリティとしてコピーすることです。たとえば、**set wlan user-priority cos** コマンドを入力する場合、CoS 値（パケットマーキング カテゴリ）がコピーされ、WLAN ユーザ プライオリティとして使用されます。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**cos**、**dscp**、**qos-group**、**wlantable** *table-map-name* の各キーワードが追加されました。

使用上のガイドライン

set dscp*dscp-value* コマンド、**set cos***cos-value* コマンドおよび **set ip precedence***precedence-value* コマンドの場合は、一般に使用されている値の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。サポートされているニーモニック名について、コマンドラインのヘルプ ストリングを表示するには、**set dscp ?** コマンドまたは **set ip precedence ?** コマンドを入力します。

set dscp cos コマンドを設定する場合は、CoS 値が 3 ビット フィールドで、DSCP 値は 6 ビット フィールドであり、CoS フィールドの 3 ビットのみが使用される点に注意してください。

set dscp qos-group コマンドを設定する場合は、次の点に注意してください。

- DSCP 値の有効な範囲は 0 ～ 63 の数字です。QoS グループの有効値の範囲は 0 ～ 99 です。
- QoS グループの値が両方の値の範囲内の場合（たとえば、44）、パケットマーキング値がコピーされ、パケットがマーク付けされます。
- QoS グループの値が DSCP の範囲を超える場合（たとえば、77）、パケットマーキング値はコピーされず、パケットはマーク付けされません。アクションは実行されません。

ポリシー マップ コンフィギュレーション モードでサービス ポリシーを作成し、インターフェイスまたは ATM 仮想回線（VC）にサービス ポリシーを付加するまで、**set qos-group** コマンドは適用できません。

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。

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。

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(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。

関連トピック

class, （874 ページ）

policy-map, （883 ページ）

show policy-map, （919 ページ）

show ap name service-policy

特定の Cisco Lightweight アクセス ポイントのサービス ポリシー情報を表示するには、**show ap name service-policy** コマンドを使用します。

show ap name *ap-name* **service-policy**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、特定の Cisco Lightweight アクセス ポイントのサービス ポリシー情報を表示する方法を示します。

```
Device# show ap name 3502b service-policy

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name dot11

特定の Cisco Lightweight アクセス ポイントに対応する 802.11a または 802.11b 設定情報を表示するには、**show ap name dot11** コマンドを使用します。

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} {**ccx**| **cdp**| **profile**| **service-policy output**| **stats**| **tsm** {**all**| *client-mac*}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
ccx	Cisco Client eXtensions（CCX）無線管理ステータス情報を表示します。
cdp	シスコ検出プロトコル（CDP）情報を表示します。
profile	802.11 プロファイルの設定と統計情報を表示します。
service-policyoutput	ダウンストリームのサービス ポリシー情報を表示します。
stats	Cisco Lightweight アクセス ポイントの統計情報を表示します。
tsm	802.11 トラフィック ストリーム メトリックの統計情報を表示します。
all	クライアントがアソシエーションを持つすべてのアクセス ポイントのリストを表示します。
client-mac	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、アクセスポイントに関連付けられたサービスポリシーを表示する方法を示します。

```
Device# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
Policy State : Installed
```

次の例では、特定のアクセス ポイントの CCX RRM 802.11 の設定を表示する例を示します。

```
Device# show ap name AP01 dot11 24ghz ccx
```

次の例では、特定のアクセス ポイントの CDP 情報を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz cdp

AP Name               AP CDP State
--------------------- --------------
AP03                  Disabled
```

次の例では、特定のアクセス ポイントの 802.11b プロファイルの設定と統計情報を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode            : GLOBAL
 802.11b Cisco AP Interference threshold              : 10 %
 802.11b Cisco AP noise threshold                     : -70 dBm
 802.11b Cisco AP RF utilization threshold            : 80 %
 802.11b Cisco AP throughput threshold                : 1000000 bps
 802.11b Cisco AP clients threshold                   : 12 clients
```

次の例では、特定のアクセスポイントのダウンストリームのサービスポリシー情報を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

次の例では、特定のアクセス ポイントの統計情報を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz stats

Number of Users................................: 0
TxFragmentCount................................: 0
MulticastTxFrameCnt............................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount.............................: 0
FrameDuplicateCount............................: 0
RtsSuccessCount................................: 0
RtsFailureCount................................: 0
AckFailureCount................................: 0
RxIncompleteFragment...........................: 0
MulticastRxFrameCnt............................: 0
FcsErrorCount..................................: 0
TxFrameCount...................................: 0
WepUndecryptableCount..........................: 0
TxFramesDropped................................: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).........: 0
  Video Bandwidth in use(% of config bw).........: 0
  Total BW in use for Voice(%)...................: 0
  Total BW in use for SIP Preferred call(%)......: 0

Load based Voice Call Stats
```

```
  Total channel MT free.......................: 0
  Total voice MT free.........................: 0
  Na Direct...................................: 0
  Na Roam.....................................: 0

WMM TSPEC CAC Call Stats
  Total num of voice calls in progress........: 0
  Num of roaming voice calls in progress......: 0
  Total Num of voice calls since AP joined....: 0
  Total Num of roaming calls since AP joined..: 0
  Total Num of exp bw requests received.......: 0
  Total Num of exp bw requests admitted.......: 0
  Num of voice calls rejected since AP joined.: 0
  Num of roam calls rejected since AP joined..: 0
  Num of calls rejected due to insufficent bw.: 0
  Num of calls rejected due to invalid params.: 0
  Num of calls rejected due to PHY rate.......: 0
  Num of calls rejected due to QoS policy.....: 0

SIP CAC Call Stats
  Total Num of calls in progress..............: 0
  Num of roaming calls in progress............: 0
  Total Num of calls since AP joined..........: 0
  Total Num of roaming calls since AP joined..: 0
  Total Num of Preferred calls received.......: 0
  Total Num of Preferred calls accepted.......: 0
  Total Num of ongoing Preferred calls........: 0
  Total Num of calls rejected(Insuff BW)......: 0
  Total Num of roam calls rejected(Insuff BW).: 0

Band Select Stats
  Num of dual band client ....................: 0
  Num of dual band client added...............: 0
  Num of dual band client expired ............: 0
  Num of dual band client replaced............: 0
  Num of dual band client detected ...........: 0
  Num of suppressed client ...................: 0
  Num of suppressed client expired............: 0
  Num of suppressed client replaced...........: 0
```

次の例では、特定のアクセスポイントに対応するすべてのクライアントのトラフィック ストリームの設定を表示する方法を示します。

```
Device# show ap name AP01 dot11 24ghz tsm all
```

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サービス品質（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* | **type control subscriber** {**all**| *class-map-name*}]

構文の説明

class-map-name	（任意）クラス マップ名。
type control subscriber	（任意）コントロールクラスマップに関する情報を表示します。
all	（任意）すべてのコントロール クラス マップに関する情報を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show class-map** コマンドの出力を示します。

```
Device# show class-map
 Class Map match-any 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-any dscp5 (id 3)
   Match ip dscp 5
```

関連トピック

class-map, （877 ページ）

show platform hardware fed switch

デバイス固有のハードウェア情報を表示するには、**show platform hardware fed switch***switch_number* コマンドを使用します。

このトピックでは、QoS 特有のオプション、つまり **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **qos** コマンドで使用可能なオプションのみについて詳しく説明します。

show platform hardware fed switch {*switch_num*| **active**| **standby**} **qos** {**afd**| {**configtype** *type*| [**asic***asic_num*]| **stats clients** {**all**| **bssid***id*| **wlanid** *id*}}| **dscp-cos counters** {**iifd_id***id*| **interface***typenumber*}| **le-info**| {**iifd_id** *id*| **interface***typenumber*}| **policerconfig** {**iifd_id***id*| **interface** *type number*}| **queue**| {**config**| {**iifd_id***id*| **interface***type number*| **internal port-type** *type* {**asic***number*[**port_num**]}}| **label2qmap**| [**aqmrepqostbl**| **iqslabeltable**| **sqslabeltable**]| {**asic***number*}| **stats**| {**iifd_id** *id*| **interface***typenumber*| **internal** {**cpupolicer**| **port-type***type***asic***number*} {**asic***number*[**port_num**]}}}| **resource**}

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するスイッチ。次の選択肢があります。 • *switch_num*：スイッチの ID。 • **active**：アクティブ スイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイ スイッチに関する情報を表示します。
qos	QoS ハードウェア情報を表示します。次のオプションの中から選択する必要があります。 • **afd**：ハードウェアの Approximate Fair Drop（AFD）の情報を表示します。 • **dscp-cos**：各ポートの DSCP-COS カウンタの情報を表示します。 • **leinfo**：論理エンティティ情報を表示します。 • **policer**：ハードウェアの QoS ポリサー情報を表示します。 • **queue**：ハードウェアのキュー情報を表示します。 • **resource**：ハードウェアのリソース情報を表示します。
afd {**config type** | **stats client** }	**config type** または **stats client** のオプションから選択する必要があります。 **config type**： • **client**：ワイヤレス クライアント情報を表示します。 • **port**：ポート固有の情報を表示します。 • **radio**：ワイヤレス無線情報を表示します。 • **ssid**：ワイヤレス SSID 情報を表示します。 **stats client**： • **all**：すべてのクライアントの統計を表示します。 • **bssid**：有効な範囲は 1 ～ 4294967295 です。 • **wlanid**：有効な範囲は 1 ~ 4294967295です。
asic*asic_num*	（任意）ASIC 番号。有効な範囲は 0 ～ 255 です。

dscp-cos counters {**iifd_id** *id* | **interface** *typenumber* }	ポートごとのDSCP-COSカウンタを表示します。**dscp-cos counters** の次のオプションから選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイス ID。有効な範囲は 1 ～ 4294967295 です。 • **interface type number**：ターゲットインターフェイス タイプおよびID。
leinfo	**dscp-cos counters** の次のオプションから選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイス ID。有効な範囲は 1 ～ 4294967295 です。 • **interface type number**：ターゲットインターフェイス タイプおよびID。
policer config	ハードウェアのポリサーに関連する設定情報を表示します。次のオプションの中から選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイス ID。有効な範囲は 1 ～ 4294967295 です。 • **interface type number**：ターゲットインターフェイス タイプおよびID。

queue{**config** {**iif_id** *id* | **interface** *typenumber* | **internal**} | **label2qmap** | **stats**}	ハードウェアのキュー情報を表示します。次のオプションの中から選択する必要があります。 • **config**：設定情報。次のオプションの中から選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイス ID。有効な範囲は 1 ～ 4294967295 です。 • **interface type number**：ターゲット インターフェイス タイプおよび ID。 • **internal**：内部キューの関連情報を表示します。 • **label2qmap**：キュー マッピング情報にハードウェア ラベルを表示します。次のオプションの中から選択できます。 • （任意）**aqmrepqostbl**：AQM REP QoS ラベル テーブルのルックアップ。 • （任意）**iqslabeltable**：IQS QoS ラベル テーブルのルックアップ。 • （任意）**sqslabeltable**：SQS およびローカル QoS ラベル テーブルのルックアップ。 • **stats**：キューの統計情報を表示します。次のオプションの中から選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイス ID。有効な範囲は 1 ～ 4294967295 です。 • **interface type number**：ターゲット インターフェイス タイプおよび ID。 • **internal** {**cpu policer** | **port_type** *port_type* **asic** *asic_num* [**port_num** *port_num*] }—Displays internal queue related information.
resource	ハードウェア リソースの使用情報を表示します。次のキーワードを入力する必要があります。**usage**

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

これは、**show platform hardware fed switch***switch_number***qos queue stats internal cpu policer** コマンドの出力例です。

```
Device#show platform hardware fed switch 3 qos queue stats internal cpu policer

                                                 (default)  (set)
QId PlcIdx  Queue Name                 Enabled    Rate     Rate       Drop
----------------------------------------------------------------------------
0    11     DOT1X Auth                  No       1000      1000          0
1    1      L2 Control                  No       500       500           0
2    14     Forus traffic               No       1000      1000          0
3    0      ICMP GEN                    Yes      200       200           0
4    2      Routing Control             Yes      1800      1800          0
5    14     Forus Address resolution    No       1000      1000          0
6    3      ICMP Redirect               No       500       500           0
7    6      WLESS PRI-5                 No       1000      1000          0
8    4      WLESS PRI-1                 No       1000      1000          0
9    5      WLESS PRI-2                 No       1000      1000          0
10   6      WLESS PRI-3                 No       1000      1000          0
11   6      WLESS PRI-4                 No       1000      1000          0
12   0      BROADCAST                   Yes      200       200           0
13   10     Learning cache ovfl         Yes      100       100           0
14   13     Sw forwarding               Yes      1000      1000          0
15   8      Topology Control            No       13000     13000         0
16   12     Proto Snooping              No       500       500           0
17   16     DHCP Snooping               No       1000      1000          0
18   9      Transit Traffic             Yes      500       500           0
19   10     RPF Failed                  Yes      100       100           0
20   15     MCAST END STATION           Yes      2000      2000          0
21   13     LOGGING                     Yes      1000      1000          0
22   7      Punt Webauth                No       1000      1000          0
23   10     Crypto Control              Yes      100       100           0
24   10     Exception                   Yes      100       100           0
25   3      General Punt                No       500       500           0
26   10     NFL SAMPLED DATA            Yes      100       100           0
27   2      SGT Cache Full              Yes      1800      1800          0
28   10     EGR Exception               Yes      100       100           0
29   16     Show frwd                   No       1000      1000          0
30   9      MCAST Data                  Yes      500       500           0
31   10     Gold Pkt                    Yes      100       100           0
```

show platform software fed switch qos

デバイス固有のソフトウェア情報を表示するには、**show platform hardware fed switch***switch_number* コマンドを使用します。

このトピックでは、**show platform software fed switch** {*switch_num* | **active** | **standby** } **qos** コマンドで使用可能な QoS 特有のオプションのみについて詳しく説明します。

show platform software fed switch {*switch number*| **active**| **standby**} **qos** {**avc**| **internal**| **label2qmap**| **nflqos**| **policer**| **policy**| **qsb**| **tablemap**| **wireless**}

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するデバイス。 • *switch_num*：スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。 • **active**：アクティブ スイッチの情報を表示します。 • **standby**：存在する場合、スタンバイ スイッチの情報を表示します。
qos	QoS ソフトウェア情報を表示します。次のいずれかのオプションを選択します。 • **avc**：Application Visibility and Control （AVC）QoS 情報を表示します。 • **internal**：内部キュー関連情報を表示します。 • **label2qmap**：キュー マップ テーブル情報へのラベルを表示します。 • **nflqos**：NetFlow QoS 情報を表示します。 • **policer**：ハードウェアの QoS ポリサー情報を表示します。 • **policy**：QoS ポリシー情報を表示します。 • **qsb**：QoS サブブロック情報を表示します。 • **tablemap**：QoS 出力および出力キューのテーブル マッピング情報を表示します。 • **wireless**：ワイヤレス QoS 情報を表示します。

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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

show platform software fed switch qos qsb

QoS サブブロック情報を表示するには、**show platform software fed switch***switch_number* **qosqsb** コマンドを使用します。

show platform software fed switch{*switch number*| **active**| **standby**}**qosqsb**{**brief**| [**all**| **type**| {**client**| *client_id*| **port**| *port_number*| **radio**| *radio_type*| **ssid**| *ssid*}]| **iif_id**| *id*| **interface**| {**Auto-Template**| *interface_number*| **BDI**| *interface_number*| **Capwap**| *interface_number*| **GigabitEthernet**| *interface_number*| **InternalInterface**| *interface_number*| **Loopback**| *interface_number*| **Null**| *interface_number*| **Port-channel**| *interface_number*| **TenGigabitEthernet**| *interface_number*| **Tunnel**| *interface_number*| **Vlan**| *interface_number*}}

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するスイッチ。 • *switch_num*：スイッチの ID を入力します。指定されたスイッチに関する情報を表示します。 • **active**：アクティブ スイッチの情報を表示します。 • **standby**：存在する場合、スタンバイ スイッチの情報を表示します。
qos qsb	QoS サブブロック ソフトウェア情報を表示します。

qsb {**brief** | **iif_id** | **interface**}	**brief** • **all**：すべてのクライアントの情報を表示します。 • **type**：指定されたターゲット タイプの qsb 情報を表示します。 ◦ **client**：ワイヤレス クライアントの QoS qsb 情報を表示します。 ◦ **port**：ポート固有の情報を表示します。 ◦ **radio**：ワイヤレス無線の QoS qsb 情報を表示します。 ◦ **ssid**：ワイヤレス ネットワークの QoS qsb 情報を表示します。 **iif_id**：iif_ID の情報を表示します。 **interface**：指定されたインターフェイスの QoS qsb 情報を表示します。 • **Auto-Template**：1 ~ 999 の自動テンプレート インターフェイス。 • **BDI**：1 ~ 16000 のブリッジ ドメイン インターフェイス。 • **Capwap**：0 ~ 2147483647 の CAPWAP インターフェイス。 • **GigabitEthernet**：0 ~ 9 の GigabitEthernet インターフェイス。 • **InternalInterface**：0 ~ 9 の内部インターフェイス。 • **Loopback**：0 ~ 2147483647 のループバック インターフェイス。 • **Null**：0 ~ 0 の null インターフェイス。 • **Port-Channel**：1 ~ 128 の port-channel インターフェイス。 • **TenGigabitEthernet**：0 ~ 9 の TenGigabitEthernet インターフェイス。 • **Tunnel**：0 ~ 2147483647 のトンネル インターフェイス。 • **VLAN**：1 ~ 4094 の VLAN インターフェイス。

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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

これは、**show platform software fed switch***switch_number***qos qsb** コマンドの出力例です。

```
Device#sh pl so fed sw 3 qos qsb interface g3/0/2

  QoS subblock information:
  Name:GigabitEthernet3/0/2 iif_id:0x0000000000007b iif_type:ETHER(146)
  qsb ptr:0xffd8573350
  Port type = Wired port
  asic_num:0 is_uplink:false init_done:true
  FRU events: Active-0, Inactive-0
  def_qos_label:0 def_le_priority:13
  trust_enabled:false trust_type:TRUST_DSCP ifm_trust_type:1
  LE priority:13 LE trans_index(in, out): (0,0)
  Stats (plc,q) export counters (in/out): 0/0
  Policy Info:
    Ingress Policy: pmap::{(0xffd8685180,AutoQos-4.0-CiscoPhone-Input-Policy,1083231504,)}
     tcg::{0xffd867ad10,GigabitEthernet3/0/2 tgt(0x7b,IN) level:0 num_tccg:4 num_child:0},
 status:VALID,SET_INHW
    Egress Policy: pmap::{(0xffd86857d0,AutoQos-4.0-Output-Policy,1076629088,)}
     tcg::{0xffd8685b40,GigabitEthernet3/0/2 tgt(0x7b,OUT) level:0 num_tccg:8 num_child:0},
 status:VALID,SET_INHW
    TCG(in,out):(0xffd867ad10, 0xffd8685b40) le_label_id(in,out):(2, 1)
  Policer Info:
    num_ag_policers(in,out)[1r2c,2r3c]: ([0,0],[0,0])
    num_mf_policers(in,out): (0,0)
    num_afd_policers:0
    [ag_plc_handle(in,out) = (0xd8688220,0)]
    [mf_plc_handle(in,out)=((nil),(nil)) num_mf_policers:(0,0)
      base:(0xffffffff,0xffffffff) rc:(0,0)]
  Queueing Info:
    def_queuing = 0, shape_rate:0 interface_rate_kbps:1000000
    Port shaper:false
    lbl_to_qmap_index:1
    Physical qparams:
     Queue Config: NodeType:Physical Id:0x40000049 parent:0x40000049 qid:0 attr:0x1 defq:0

        PARAMS: Excess Ratio:1 Min Cir:1000000 QBuffer:0
        Queue Limit Type:Single Unit:Percent Queue Limit:44192
        SHARED Queue
```

show wireless client calls

デバイス のアクティブなコールまたは拒否されたコールの合計数を表示するには、特権 EXEC モードで **show wireless client calls** コマンドを使用します。

show wireless client calls {**active** | **rejected**}

構文の説明

active	アクティブなコールが表示されます。
rejected	拒否されたコールが表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless client calls** コマンドの出力例を示します。

```
デバイス# show wireless client calls active

TSPEC Calls:

------------------------------------------------------------------------------
MAC Address     AP Name             Status               WLAN  Authenticated
------------------------------------------------------------------------------
0000.1515.000f    AP-2           Associated             1  Yes

SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

特定の帯域（2.4 Ghz または 5 Ghz）のアクティブなコールまたは拒否されたコールの合計数を表示するには、特権 EXEC モードで **show wireless client dot11** コマンドを使用します。

show wireless client dot11 {**24ghz** | **5ghz**} **calls** {**active** | **rejected**}

構文の説明

24ghz	802.11b/g ネットワークを表示します。
5ghz	802.11a ネットワークを表示します。
calls	ワイヤレス クライアントのコールを表示します。
active	アクティブなコールが表示されます。
rejected	拒否されたコールが表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless client dot11** コマンドの出力例を示します。

```
Device# show wireless client dot11 5ghz calls active

 TSPEC Calls:
------------------


SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client mac-address（コール制御）

クライアントに関連するコール制御情報を表示するには、特権 EXEC モードで **show wireless client mac-address** コマンドを使用します。

show wireless client mac-address *mac-address* **call-control call-info**

構文の説明

mac-address	クライアントの MAC アドレス。
call-controlcall-info	クライアントに関するコール制御と IP 関連の情報を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、クライアントに関するコール制御および IP に関する情報を表示する方法を示します。

```
Device# show wireless client mac-address  30e4.db41.6157 call-control call-info
Client MAC Address        : 30E4DB416157

Call 1 Statistics

Uplink IP Address         : 209.165.200.225
Downlink IP Address       : 209.165.200.226
Uplink Port               : 29052
Downlink Port             : 27538
Call ID                   : c40acb4d-3b3b0.3d27da1e-356bed03
Called Party              : sip:1011
Calling Party             : sip:1012
Priority                  : 6
Call On Hold              : false
Call Duration             : 30

Call 2 Statistics

No Active Call
```

show wireless client mac-address（TCLAS）

TCLAS およびユーザ プライオリティに関する情報を表示するには、特権 EXEC モードで **showwirelessclientmac-address** コマンドを使用します。

show wireless client mac-address *mac-address* **tclas**

構文の説明

mac-address	クライアントの MAC アドレス。
tclas	TCLAS およびクライアントに関するユーザ プライオリティ関連の情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

この例は、クライアントの TCLAS およびユーザ プライオリティ関連の情報を表示する方法を示しています。

```
Device# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr    SrcPort DstPort Proto
-------------------------------------------------------------------------------
```

```
30e4.db41.6157    4   4   95 167838052       2164326668      5060     5060      6
30e4.db41.6157    6   1   31 0               2164326668      0        27538    17
```

show wireless client voice diagnostics

ワイヤレス クライアントの音声診断パラメータを表示するには、特権 EXEC モードで **show wireless client voice diagnostics** コマンドを使用します。

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rssi** | **status** | **tspec**}

構文の説明

qos-map	QoS および DSCP マッピングに関する情報と 4 つのキュー（VO、VI、BE、BK）それぞれのパケット統計を表示します。各種 DSCP 値も表示されます。
roam-history	既知の各クライアントの直前の 3 つのローミング履歴に関する情報を表示します。出力にはタイムスタンプ、ローミングに関連するアクセス ポイント、ローミングの理由が含まれ、ローミングに失敗した場合には失敗の理由も含まれます。
rssi	音声診断がイネーブルである場合に、直前の 5 秒間のクライアントの RSSI 値を表示します。
status	クライアントの音声診断の状態を表示します。
tspec	TSPEC クライアントに対して有効になっている音声診断を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デバッグ音声診断は、音声診断を実行するにはイネーブルにする必要があります。

次は、**show wireless client voice diagnostics status** コマンドの出力例です。

```
Device# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show policy-map

着信トラフィックの分類基準を定義するサービス品質（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。

show policy-map [*policy-map-name*| **interface** *interface-id*]

show policy-map interface{**Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output**

show policy-map type control subscriber detail

show policy-map interface wireless{**ap name** *ap_name* | **client mac***mac_address* | **radio type**{**24ghz**| **5ghz**} **ap name***ap_name* | **ssid name***ssid_name*{**ap name***ap_name* | **radio type**{**24ghz**| **5ghz**} **ap name***ap_name*}}

構文の説明

policy-map-name	（任意）ポリシーマップの名前。
interface *interface-id*	（任意）インターフェイスに適用された入力ポリシーと出力ポリシーの統計情報と設定を表示します。
type control subscriber detail	（任意）QoS ポリシーのタイプと統計情報を特定します。
ap name *ap_name*	アクセス ポイントの SSID ポリシー設定を表示します。
client mac*mac_address*	すべてのクライアント ターゲットのポリシーに関する情報を表示します。
radio type{**24ghz**| **5ghz**	指定された無線タイプのアクセス ポイントのポリシー設定を表示します。
ssid name*ssid_name*	SSID のポリシー設定を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	The **interface** *interface-id* keyword was added.

使用上のガイドライン

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。

（注） **control-plane**、**session**、および **type** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。表示されている統計情報は無視してください。

次に、**show policy-map interface** コマンドの出力例を示します。

```
Device# show policy-map interface gigabitethernet1/0/48GigabitEthernet1/0/48

  Service-policy output: port_shape_parent

    Class-map: class-default (match-any)
      191509734 packets
      Match: any
      Queueing

      (total drops) 524940551420
      (bytes output) 14937264500
      shape (average) cir 250000000, bc 2500000, be 2500000
      target shape rate 250000000

      Service-policy : child_trip_play

        queue stats for all priority classes:
          Queueing
          priority level 1

          (total drops) 524940551420
          (bytes output) 14937180648

        queue stats for all priority classes:
          Queueing
          priority level 2

          (total drops) 0
          (bytes output) 0

        Class-map: dscp56 (match-any)
          191508445 packets
          Match:  dscp cs7 (56)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Priority: Strict,

          Priority Level: 1
          police:
              cir 10 %
              cir 25000000 bps, bc 781250 bytes
            conformed 0 bytes; actions: >>>>>counters not supported
```

```
  transmit
exceeded 0 bytes; actions:
  drop
conformed 0000 bps, exceeded 0000 bps  >>>>>counters not supported
```

関連トピック

policy-map, （883 ページ）

show wlan

WLAN パラメータを表示するには、**show wlan** コマンドを使用します。

show wlan {**all** | **id** *wlan-id*| **name** *wlan-name* | **summary**}

構文の説明

all	すべての設定済み WLAN のパラメータのサマリーを表示します。リストは WLAN ID の昇順に表示されます。
id *wlan-id*	無線 LAN の識別子を指定します。範囲は 1 ～ 512 です。
name *wlan-name*	WLAN プロファイル名を指定します。名前は 1 ～ 32 文字です。
summary	WLAN に設定されているパラメータのサマリーを表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、デバイスに設定されている WLAN のサマリーを表示する例を示します。

```
Device# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                                VLAN Status
-------------------------------------------------------------------------------------
```

```
45   test-wlan                        test-wlan-ssid                 1    UP
```

次に、特定の WLAN に設定されているパラメータのサマリーを表示する例を示します。

```
Device# show wlan name test-wlan
WLAN Identifier                                 : 45
Profile Name                                    : test-wlan
Network Name (SSID)                             : test-wlan-ssid
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Maximum number of Associated Clients            : 0
AAA Policy Override                             : Disabled
Network Admission Control
  NAC-State                                     : Disabled
Number of Active Clients                        : 0
Exclusionlist Timeout                           : 60
Session Timeout                                 : 1800 seconds
CHD per WLAN                                    : Enabled
Webauth DHCP exclusion                          : Disabled
Interface                                       : default
Interface Status                                : Up
Multicast Interface                             : test
WLAN IPv4 ACL                                   : test
WLAN IPv6 ACL                                   : unconfigured
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : ap-mac
DHCP Option 82 Ascii Mode                       : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Service Policy - Output
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Client Service Policy
  Input  Policy Name                            : unknown
  Output Policy Name                            : unknown
WifiDirect                                      : Disabled
WMM                                             : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Gratuitous ProbeResponse (GPR)            : Disabled
CCX - Diagnostics Channel Capability            : Disabled
Dot11-Phone Mode (7920)                         : Invalid
Wired Protocol                                  : None
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Enabled
            PSK                                 : Disabled
            CCKM                                : Disabled
```

```
    IP Security                                 : Disabled
    IP Security Passthru                        : Disabled
    L2TP                                        : Disabled
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Auto Anchor                                 : Disabled
    Sticky Anchoring                            : Enabled
    Cranite Passthru                            : Disabled
    Fortress Passthru                           : Disabled
    PPTP                                        : Disabled
    Infrastructure MFP protection               : Enabled
    Client MFP                                  : Optional
    Webauth On-mac-filter Failure               : Disabled
    Webauth Authentication List Name            : Disabled
    Webauth Parameter Map                       : Disabled
    Tkip MIC Countermeasure Hold-down Timer     : 60
Call Snooping                                   : Disabled
Passive Client                                  : Disabled
Non Cisco WGB                                   : Disabled
Band Select                                     : Disabled
Load Balancing                                  : Disabled
IP Source Guard                                 : Disabled
Netflow Monitor                                 : test
        Direction                               : Input
        Traffic                                 : Datalink

Mobility Anchor List
IP Address
-----------
```

trust device

インターフェイスに接続されているサポート デバイスに対する信頼を設定するには、インターフェイス コンフィギュレーション モードで **trust device** コマンドを使用します。接続デバイスに対する信頼を無効にするには、このコマンドの **no** 形式を使用します。

trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

no trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

構文の説明

cisco-phone	Cisco IP Phone を設定します。
cts	Cisco TelePresence System を設定します。
ip-camera	Video Surveillance IP カメラ（IPVSC）を設定します。
media-player	Cisco Digital Media Player（DMP）を設定します。

コマンド デフォルト

信頼はディセーブルに設定

コマンド モード

インターフェイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

trust device コマンドは、次のタイプのインターフェイスに使用します。

- **Auto**：自動テンプレート インターフェイス
- **Capwap**：Capwap トンネル インターフェイス
- **GigabitEthernet**：Gigabit Ethernet IEEE 802
- **GroupVI**：グループ仮想インターフェイス
- **Internal Interface**：内部インターフェイス
- **Loopback**：ループバック インターフェイス
- **Null**：ヌル インターフェイス
- **Port-channel**：イーサネット チャネル インターフェイス
- **TenGigabitEthernet**：10 ギガビット イーサネット
- **Tunnel**：トンネル インターフェイス
- **Vlan**：Catalyst VLAN
- **range**：**interface range** コマンド

例

次に、インターフェイス GigabitEthernet 1/0/1 で Cisco IP Phone の信頼を設定する例を示します。

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# trust device cisco-phone
```

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

第 XV 部

Radio Resource Management

- 無線リソース管理コマンド，927 ページ

第 16 章

無線リソース管理コマンド

- airtime-fairness dot11 mode（apgroup），929 ページ
- airtime-fairness dot11 optimization（apgroup），930 ページ
- airtime-fairness dot11 policy，931 ページ
- airtime-fairness policy（wlan），932 ページ
- ap dot11 rf-profile，933 ページ
- ap dot11 rrm，934 ページ
- ap dot11 rrm ccx，936 ページ
- ap dot11 rrm channel，937 ページ
- ap dot11 24ghz rrm channel cleanair-event rogue-contribution，938 ページ
- ap dot11 24ghz または 5ghz rrm channel dca add，939 ページ
- ap dot11 24ghz または 5ghz rrm channel dca remove，940 ページ
- ap dot11 5ghz rrm channel dca chan-width-11n，941 ページ
- ap dot11 rrm coverage，942 ページ
- ap dot11 rrm group-member，943 ページ
- ap dot11 rrm monitor，944 ページ
- ap dot11 rrm profile，945 ページ
- ap dot11 rrm tpc-threshold，946 ページ
- ap dot11 rrm txpower，947 ページ
- ap dot11 airtime-fairness mode，948 ページ
- ap dot11 airtime-fairness policy-name，949 ページ
- ap group，950 ページ

- ap name dot11 airtime-fairness mode, 951 ページ
- ap name dot11 airtime-fairness optimization, 952 ページ
- ap name no dot11 airtime-fairness wlan-name policy-name, 953 ページ
- ap name dot11 airtime-fairness wlan-name policy, 954 ページ
- band-select client, 955 ページ
- band-select cycle, 955 ページ
- band-select expire, 956 ページ
- band-select probe-response, 957 ページ
- channel, 958 ページ
- channel foreign, 959 ページ
- チャネル幅, 960 ページ
- coverage, 960 ページ
- coverage exception, 961 ページ
- coverage level, 962 ページ
- clear wireless airtime-fairness statistics, 963 ページ
- dot11n-only, 963 ページ
- load-balancing, 964 ページ
- high-density clients count, 965 ページ
- high-density clients wlan, 966 ページ
- high-density multicast data-rate, 967 ページ
- high-density rx-sop threshold, 968 ページ
- rate, 969 ページ
- rate mcs, 970 ページ
- trap threshold, 970 ページ
- tx-power, 971 ページ
- tx-power v1 threshold, 972 ページ
- no ap dot11 airtime-fairness policy-name, 973 ページ
- remote-lan, 974 ページ
- rf-profile dot11 24ghz, 974 ページ
- rf-profile dot11 5ghz, 975 ページ
- show ap airtime-fairness ap-group, 976 ページ

- show ap airtime-fairness (ap)，977 ページ
- show ap airtime-fairness（無線別），977 ページ
- show ap airtime-fairness policy（すべて），978 ページ
- show ap airtime-fairness wlan，979 ページ
- show ap dot11 24ghz，979 ページ
- show ap dot11 5ghz，981 ページ
- show ap dot11 airtime-fairness（無線帯域），982 ページ
- show ap dot11 24ghz rf-profile summary，983 ページ
- show ap dot11 5ghz rf-profile summary，984 ページ
- show ap name dot11 airtime-fairness summary，985 ページ
- show ap name dot11 airtime-fairness policy statistics，985 ページ
- show ap name dot11 airtime-fairness wlan name statistics，986 ページ
- show ap rf-profile summary，987 ページ
- show ap rf-profile name，988 ページ
- show wireless mobility controller ap，990 ページ
- シャットダウン，990 ページ
- wlan，991 ページ

airtime-fairness dot11 mode（apgroup）

AP グループの ATF を設定するには、AP グループ サブモードで **airtime-fairness dot11 mode** コマンドを使用します。AP グループの ATF を無効にするには、このコマンドの **no** 形式を使用します。

airtime-fairness dot11{**24ghz**| **5ghz**} **mode**{**enforce-policy**| **monitor**}

no airtime-fairness dot11{**24ghz**| **5ghz**} **mode**{**enforce-policy**| **monitor**}

構文の説明

24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
enforce-policy	強制ポリシー モードで Air Time Fairness を設定します。
monitor	モニタ モードで Air Time Fairness を設定します。

コマンド デフォルト

なし

コマンド モード

config apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP グループの ATF を設定する例を示します。

```
Device#configure terminal
Deviceconfig# ap group testap
Deviceconfig-apgroup# airtime-fairness dot11 24ghz mode monitor
```

airtime-fairness dot11 optimization（apgroup）

AP グループの ATF 最適化を設定するには、**airtime-fairness dot11 optimization** コマンドを使用します。AP グループの ATF を無効にするには、このコマンドの **no** 形式を使用します。

airtime-fairness dot11 {**24ghz**| **5ghz**} **optimization**

no airtime-fairness dot11 {**24ghz**| **5ghz**} **optimization**

構文の説明

24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。

コマンド デフォルト

なし

コマンド モード

config apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP グループの ATF 最適化を設定する例を示します。

```
Device#configure terminal
Deviceconfig# ap group testap
Deviceconfig-apgroup# airtime-fairness dot11 24ghz optimization
```

airtime-fairness dot11 policy

WLAN AP グループでグローバルに適用されているポリシーをオーバーライドするには、**airtime-fairness dot11 policy** コマンドを使用します。適用されているポリシーのオーバーライドを無効にするには、コマンドの **no** 形式を使用します。

airtime-fairness dot11 {**24ghz**| **5ghz**} **policy***policy-name*

no airtime-fairness dot11 {**24ghz**| **5ghz**} **policy***policy-name*

構文の説明

24ghz	2.4 GHz Air Time Fairness ポリシーを設定します。
5ghz	5 GHz Air Time Fairness ポリシーを設定します。
policy-name	割り当てる Air Time Fairness ポリシーの名前。

コマンド デフォルト

なし

コマンド モード

config wlan apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、WLAN AP グループで適用されているポリシーをオーバーライドする例を示します。

```
Deviceconfig#ap group testapgroup
Device(config-apgroup)# wlan testwlan
Device(config-wlan-apgroup)# airtime-fairness dot11 24ghz policy testpolicy
```

airtime-fairness policy（wlan）

WLAN の ATF ポリシーを設定するには、**airtime-fairness policy** コマンドを使用します。

airtime-fairness policy*policy-name*

構文の説明

policy-name	ポリシー名を入力します。

コマンド デフォルト

なし

コマンド モード

config wlan

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、WLAN の ATF ポリシーを設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wlan wlan-name
Device(config-wlan)#airtime-fairness policy policy-name
```

ap dot11 rf-profile

選択した帯域の RF プロファイルを設定するには、**ap dot11 rf-profile** コマンドを使用します。RF 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。

ap dot11 {**24GHz | 5GHz**} **rf-profile** *profile name*

構文の説明

24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
profile name	RF プロファイルの名前。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし
次に、選択した帯域の RF プロファイルを設定する例を示します。

```
Device#ap dot11 24GHz rf-profile doctest
```

ap dot11 rrm

802.11 デバイスの無線リソース管理の基本設定および詳細設定を指定するには、**apdot11rrm** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **rrm** {**ccx location-measurement** *sec*| **channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**| **outdoor-ap-dca**}| **coverage** {**data fail-percentage** *pct*| **data packet-count** *count*| **data rssi-threshold** *threshold*}| **exception global** *percentage*| **level global** *number*| **voice** {**fail-percentage** *percentage*| **packet-count** *number*| **rssi-threshold** *threshold*}}

構文の説明

ccx	高度な（RRM）802.11 CCX オプションを設定します。
location-measurement	802.11 CCX クライアント ロケーション測定（秒単位）を指定します。値の範囲は 10 ～ 32400 秒です。
channel	高度な 802.11 チャネル割り当てパラメータを設定します。
cleanair-event	CleanAir のイベント駆動型 RRM パラメータを設定します。
dca	802.11 動的チャネル割り当てアルゴリズムのパラメータを設定します。
device	802.11 チャネル割り当てでの永続型非 Wi-Fi デバイス回避を設定します。
foreign	チャネル割り当てでの外部 AP の 802.11 干渉回避を有効にします。
load	チャネル割り当てでのシスコの AP の 802.11 負荷回避を有効にします。
noise	チャネル割り当てでの 802.11a 以外のノイズ回避を有効にします。

outdoor-ap-dca	屋外 AP の 802.11 DCA リスト オプションを設定します。
coverage	802.11 カバレッジ ホール検出を設定します。
datafail-percentage*pct*	アップリンク データ パケットの 802.11 カバレッジ障害率しきい値を設定します。範囲は 1 ～ 100 です。
datapacket-count*count*	アップリンク データ パケットの 802.11 カバレッジ最小障害数しきい値を設定します。
datarssi-threshold*threshold*	音声パケットの 802.11 最小受信カバレッジ レベルを設定します。
exceptionglobal*percentage*	802.11 シスコ AP カバレッジ例外レベルを設定します。範囲は 0 ～ 100 % です。
levelglobal*number*	802.11 シスコ AP クライアント最小例外レベルを設定します（1 ～ 75 クライアント）。
voice	音声パケットの 802.11 カバレッジ ホール検出を設定します。
fail-percentage*percentage*	音声パケットの 802.11 カバレッジ障害率しきい値を設定します。
packet-count*number*	音声パケットの 802.11 カバレッジ最小アップリンク障害数しきい値を設定します。
rssi-threshold*threshold*	音声パケットの 802.11 最小受信カバレッジ レベルを設定します。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、802.11a 帯域と 802.11b 帯域の両方に適用されます。ただし、パラメータの設定には適切なコマンドを選択する必要があります。

次に、さまざまな RRM 設定を指定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm ?
  ccx             Configure Advanced(RRM) 802.11a CCX options
  channel         Configure advanced 802.11a channel assignment parameters
  coverage        802.11a Coverage Hole Detection
  group-member    Configure members in 802.11a static RF group
  group-mode      802.11a RF group selection mode
  logging         802.11a event logging
  monitor         802.11a statistics monitoring
  ndp-type        Neighbor discovery type Protected/Transparent
  profile         802.11a performance profile
  tpc-threshold   Configures the Tx Power Control Threshold used by RRM for auto
                  power assignment
  txpower         Configures the 802.11a Tx Power Level
```

ap dot11 rrm ccx

2.4 GHz デバイスおよび 5 GHz デバイスの無線リソース管理 CCX オプションを設定するには、**ap dot11 rrm ccx** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**}**rrm ccx location-measurement** *interval*

構文の説明

location-measurement *interval*	CCX クライアント ロケーション測定間隔値を指定します。値の範囲は 10 ～ 32400 秒です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、5 GHz デバイスの CCX ロケーション測定間隔を設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm ccx location-measurement 10
```

ap dot11 rrm channel

2.4 GHz デバイスおよび 5 GHz デバイスの無線リソース管理チャネルを有効にするには、**apdot11rrmchannel** コマンドを使用します。2.4 GHz デバイスおよび 5 GHz デバイスの無線リソース管理を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**}**rrm channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**}

no ap dot11 {**24ghz**| **5ghz**}**rrm channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**}

構文の説明

cleanair-event	CleanAir のイベント駆動型 RRM パラメータを指定します。
dca	802.11 動的チャネル割り当てアルゴリズムのパラメータを指定します。
device	802.11 チャネル割り当てでの永続型非 Wi-Fi デバイス回避を指定します。
foreign	チャネル割り当てでの外部 AP の 802.11 干渉回避を有効にします。
load	チャネル割り当てでのシスコの AP の 802.11 負荷回避を有効にします。
noise	チャネル割り当てでの 802.11a 以外のノイズ回避を有効にします。

コマンド デフォルト

なし（インターフェイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次の例は、**チャネル**の使用可能なすべてのパラメータを示しています。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 24ghz rrm channel ?
  cleanair-event  Configure cleanair event-driven RRM parameters
  dca             Config 802.11b dynamic channel assignment algorithm
                  parameters
  device          Configure persistent non-WiFi device avoidance in the 802.11b
                  channel assignment
  foreign         Configure foreign AP 802.11b interference avoidance in the
                  channel assignment
  load            Configure Cisco AP 802.11b load avoidance in the channel
                  assignment
  noise           Configure 802.11b noise avoidance in the channel assignment
```

ap dot11 24ghz rrm channel cleanair-event rogue-contribution

CleanAir イベント駆動型 Radio Resource Management（RRM; 無線リソース管理）の不正寄与パラメータを設定するには、**ap dot11 24ghz rrm channel cleanair-event rogue-contribution** コマンドを使用します。

ap dot11 24ghz rrm channel cleanair-event rogue-contribution duty-cycle *threshold-value*

構文の説明

duty-cycle	イベント駆動型 RRM の不正寄与デューティ サイクルを設定します。
threshold-value	ED-RRM 不正寄与デューティ サイクルのしきい値をカスタマイズします。有効な値の範囲は 1 ~ -99 % です。

コマンド デフォルト

不正寄与デューティ サイクルは設定されていません。

コマンド履歴

リリース	変更内容
16.1	このコマンドが導入されました。

使用上のガイドライン

次のコマンドは、イベント駆動型 RRM の不正寄与デューティ サイクルを設定します。

例

次に、CleanAir イベント駆動型 RRM の不正寄与パラメータを設定する例を示します。

```
Cisco Controller(config)# ap dot11 24ghz rrm channel cleanair-event rogue-contribution
duty-cycle 1
```

ap dot11 24ghz または 5ghz rrm channel dca add

2.4 GHz デバイスまたは 5 GHz デバイスの DCA チャネル リストに非デフォルトの無線リソース管理 DCA チャネルを追加するには、**apdot11** {**24ghz**| **5ghz** } **rrm channel dca add** コマンドを使用します。DCA リストからデフォルトのチャネルを削除するには、このコマンドの **no** 形式を使用します。DCA チャネル リストには、使用する国に適合する標準チャネルが含まれています。たとえば、規制デフォルト チャネル リストにはチャネル 1、6、11 が含まれています。

ap dot11 [**24ghz**| **5ghz**]**rrm channel dca add** *number*

no ap dot11 [**24ghz**| **5ghz**]**rrm channel dca add** *number*

構文の説明

number	DCA チャネル番号。

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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、**ap dot11 24ghz rrm channel dca add 10** コマンドを使用して 2.4 GHz デバイスの DCA リストに非デフォルトの無線リソース管理 DCA チャネルを追加する例を示します。

```
Device(config)# ap dot11 24ghz rrm channel dca add 10
```

ap dot11 24ghz または 5ghz rrm channel dca remove

2.4 GHz デバイスまたは 5 GHz デバイスの DCA チャネル リストからデフォルトの無線リソース管理 DCA チャネルを削除するには、**ap dot11**{**24ghz** | **5ghz**} **rrm channel dcaremove***number* コマンドを使用します。デフォルトの DCA チャネルを DCA チャネル リストに戻すには、このコマンドの **no** 形式を使用します。

ap dot11 [**24ghz**| **5ghz**] **rrm channel dca remove** *number*

no ap dot11 [**24ghz**| **5ghz**] **rrm channel dca remove** *number*

構文の説明

number	無線リソース管理 DCA チャネルを指定します。

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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、**ap dot11 24ghz rrm channel dca remove** コマンドを使用して 2.4 GHz デバイスの DCA リストからデフォルトの無線リソース管理 DCA チャネルを削除する例を示します。

```
Device(config)#ap dot11 24ghz rrm channel dca remove 11
```

ap dot11 5ghz rrm channel dca chan-width-11n

5 GHz 帯域のすべての 802.11n 無線に対して DCA チャネル幅を設定するには、**apdot115ghzrrmchanneldcachan-width-11n***width* コマンドを使用します。5 GHz 帯域のすべての 802.11n 無線に対して DCA チャネル幅を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghzrrm channel dca chan-width-11n {**20**|**40**}

noap dot11 5ghzrrm channel dca chan-width-11n {**20**|**40**}

構文の説明

chan-width-11n	5 GHz 帯域のすべての 802.11n 無線に対して DCA チャネル幅を指定します。
20	802.11n 無線のチャネル幅を 20 MHz に設定します。
40	802.11n 無線のチャネル幅を 40 MHz に設定します。

コマンド デフォルト

デフォルトのチャネル幅は 20 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、**ap dot11 5ghz rrm channel dca chan-width-11n** コマンドを使用して、802.11n 無線のチャネル幅を 40 MHzに設定する例を示します。

```
Device(config)#ap dot11 5ghz rrm channel dca chan-width-11n 40
```

ap dot11 rrm coverage

802.11 カバレッジ ホール検出を有効にするには、**apdot11rrmcoverage** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**}**rrm coverage** [**data** {**fail-percentage** *percentage*| **packet-count** *count*| **rssi-threshold** *threshold*}| **exceptional global** *value*| **level global** *value*| **voice** {**fail-percentage** *percentage*| **packet-count** *packet-count*| **rssi-threshold** *threshold*}]

構文の説明

data	802.11 カバレッジ ホール検出のデータ パケットを指定します。
fail-percentage*percentage*	アップリンク データ パケットの 802.11 カバレッジ障害率しきい値を指定します。範囲は 1 ～ 100 です。
packet-count*count*	アップリンク データ パケットの 802.11 カバレッジ最小障害数しきい値を指定します。
rssi-threshold*threshold*	音声パケットの 802.11 最小受信カバレッジ レベルを指定します。
exceptionalglobal*value*	802.11 シスコ AP カバレッジ例外レベルを指定します。範囲は 0 ～ 100 % です。
levelglobal*value*	802.11 シスコ AP クライアント最小例外レベルを指定します（1 ～ 75 クライアント）。
voice	音声パケットの 802.11 カバレッジ ホール検出を指定します。
fail-percentage*percentage*	音声パケットの 802.11 カバレッジ障害率しきい値を指定します。
packet-count*packet-count*	音声パケットの 802.11 カバレッジ最小アップリンク障害数しきい値を指定します。
rssi-threshold*threshold*	音声パケットの 802.11 最小受信カバレッジ レベルを指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

カバレッジ ホール検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセスポイントがあるかどうかを、アクセスポイントから受信したデータに基づいてデバイスが自動的に判断します。

5 秒間で失敗したパケットの数と割合の両方が、**ap dot11 {24ghz | 5ghz} rrm coverage packet-count** コマンドと **ap dot11 {24ghz | 5ghz} rrm coverage fail-percentage** コマンドに入力された値を超える場合、クライアントは事前アラーム状態と判断されます。デバイスは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。失敗したクライアントの数と割合の両方が、90 秒以上にわたって、**ap dot11 {24ghz | 5ghz} rrm coverage level-global** コマンドと **ap dot11 {24ghz | 5ghz} rrm coverage exceptional-global** コマンドで入力した値以上になると、カバレッジホールが検出されます。デバイスは、カバレッジホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジホールを解消します。

次に、5 GHz 帯域で データの RSSI しきい値を設定する例を示します。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#ap dot11 5ghz rrm coverage data rssi-threshold -80
```

ap dot11 rrm group-member

802.11 静的 RF グループのメンバを設定するには、**apdot11rrmgroup-member** コマンドを使用します。メンバを削除するには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**}**rrm group-member** *controller-name controller-ip*

no ap dot11 {**24ghz**| **5ghz**}**rrm group-member** *controller-name controller-ip*

構文の説明

controller-name	追加するコントローラの名前を指定します。
controller-ip	追加するコントローラの IP アドレスを指定します。

コマンド デフォルト

なし インターフェイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、5 GHz 自動 RF グループにコントローラを追加する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm group-member ABC 10.1.1.1
```

ap dot11 rrm monitor

802.11 帯域統計情報をモニタするには、**apdot11rrmmonitor** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**}**rrm monitor** {**channel-list**| {**all**| **country**| **dca**}| **coverage**| **load**| **noise**| **signal**}

no ap dot11 {**24ghz**| **5ghz**}**rrm monitor** {**channel-list**| **coverage**| **load**| **noise**| **signal**}

構文の説明

channel-list	802.11 ノイズ/干渉/不正モニタリング チャネル リストを設定します。
all	すべてのチャネルをモニタすることを指定します。
country	設定された国コードで使用するチャネルをモニタすることを指定します。
dca	動的チャネル割り当てで使用されるチャネルをモニタすることを指定します。
coverage	802.11 カバレッジ測定間隔を指定します。値の範囲は 60 ～ 3600（秒単位）です。
load	802.11 負荷測定間隔を指定します。値の範囲は 60 ～ 3600（秒単位）です。
noise	802.11 ノイズ測定間隔（チャネル スキャン間隔）を指定します。値の範囲は 60 ～ 3600（秒単位）です。
signal	802.11 信号測定間隔（ネイバー パケット周波数）を指定します。値の範囲は 60 ～ 3600（秒単位）です。

コマンド モード

なしインターフェイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、すべての 5GHz 帯域チャネルのモニタリングを有効にする例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm monitor channel-list all
```

ap dot11 rrm profile

サポートされている 802.11 ネットワークの Cisco Lightweight アクセス ポイント プロファイルを設定するには、**apdot11rrmprofile** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**}**rrm profile** {**customize**| **foreign** *value*| **noise** *value*| **throughput** *value*| **utilization** *value*}

構文の説明

customize	パフォーマンス プロファイルを有効にします。
foreign*value*	802.11 外部 802.11 干渉しきい値を指定します。範囲は 0 ～ 100 % です。
noise*value*	802.11 外部ノイズしきい値を指定します。範囲は -127 ～ 0 dBm です。
throughput*value*	802.11a シスコ AP スループットしきい値を指定します。値の範囲は 1000 ～ 10000000 バイト/秒です。
utilization*value*	802.11a RF 使用率しきい値を指定します。範囲は 0 ～ 100 % です。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、ノイズ パラメータのしきい値を設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm profile noise -50
```

ap dot11 rrm tpc-threshold

自動電力割り当てのために RRM によって使用される TX 電力制御しきい値を設定するには、**apdot11rrmtpc-threshold** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**}**rrm tpc-threshold** *value*

no ap dot11 {**24ghz**| **5ghz**}**rrm tpc-threshold**

構文の説明

value	電力値を指定します。範囲は -80 ～ -50 です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、自動電力割り当てのためにRRMによって使用されるTX電力制御しきい値を設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm tpc-threshold -60
```

ap dot11 rrm txpower

802.11 TX 電力レベルを設定するには、**apdot11rrmtxpower** コマンドを使用します。802.11 TX 電力レベルを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**| **5ghz**} **rrm txpower** {**auto**| **max** *powerLevel*| **min** *powerLevel*| **once**| *power-level*}

noap dot11 {**24ghz**| **5ghz**} **rrm txpower** {**auto**| **max** *powerLevel*| **min** *powerLevel*| **once**| *power-level*}

構文の説明

auto	自動 RF を有効にします。
max*powerLevel*	最大自動 RF TX 電力を設定します。範囲は -10 ～ -30 です。
min*powerLevel*	最小自動 RF TX 電力を設定します。範囲は -10 ～ -30 です。
once	ワンタイム自動 RF を有効にします。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	このコマンドの **no** 形式が導入されました。

使用上のガイドライン

なし。

次に、ワンタイム自動 RF を有効にする例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm txpower once
```

ap dot11 airtime-fairness mode

Air Time Fairness を強制ポリシー モードまたはモニタ モードで有効にするには、**apdot11airtime-fairness mode** コマンドを使用します。Air Time Fairness の強制ポリシー モードまたはモニタ モードを無効にするには、このコマンドの **no** 形式を使用します。

apdot11{**24ghz**| **5ghz**}**airtime-fairness mode**{**enforce-policy**| **monitor**}

noapdot11{**24ghz**| **5ghz**}**airtime-fairness mode**{**enforce-policy**| **monitor**}

構文の説明

24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
enforce-policy	強制ポリシー モードで Air Time Fairness を設定します。
monitor	モニタ モードで Air Time Fairness を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次の例は、**Air Time Fairness モード**の使用可能なすべてのパラメータを示しています。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 24ghz airtime-fairness mode ?
 enforce-policy  Configure airtime-fairness in enforce-policy mode
 monitor         Configure airtime-fairness in monitor mode
```

ap dot11 airtime-fairness policy-name

新しい Air Time Fairness（ATF）ポリシーを作成するには、**ap dot11 airtime-fairness policy-name** コマンドを使用します。

ap dot11 airtime-fairness policy-name*policy-namepolicy-id*

構文の説明

policy-name	ATF ポリシー名を入力します。
policy-id	新しいポリシーを作成するための ATF ポリシー ID を入力します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	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 ATF ポリシーには、ポリシー ウェイト値が必要です。ポリシー ウェイトを追加するには、config-airtime-fairness ポリシー モードで **policy weight** コマンドを使用します。ポリシー ウェイトを追加しない場合は、デフォルト値の 10 が適用されます。ポリシー ウェイト追加の詳細については、policy-weight, （950 ページ）を参照してください。
次に例を示します。

```
Device#ap dot11 airtime-fairness policy-name testpolicy 12
```

policy-weight

Air Time Fairness（ATF）ポリシーにポリシー ウェイトを適用するには、**policy-weight** コマンドを使用します。

policy-weight*policy-weight*

構文の説明

policy-weight	ATF ポリシーのポリシー ウェイト。範囲は 5 ～ 100 です。デフォルト値は 10 です。

コマンド デフォルト

なし

コマンド モード

config-airtime-fairness policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

WLAN にポリシーを適用しない場合、ポリシー ウェイト 10 のデフォルト ポリシー（ID 0）が自動的に適用されます。ATF ポリシー作成の詳細については、ap dot11 airtime-fairness policy-name,（949 ページ）を参照してください。

次に、ATF ポリシーにポリシー ウェイトを適用する例を示します。

```
Device#ap dot11 airtime-fairness policy-name testpolicy 12
Device(config-airtime-fairness policy)# policy-weight 35
```

ap group

AP グループを設定するには、**ap group** コマンドを使用します。

ap group *group-name*

構文の説明

group-name	AP グループの名前

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし
次に、AP グループを設定する例を示します。

```
Deviceconfig# ap group docgroup
```

ap name dot11 airtime-fairness mode

特定の AP の Air Time Fairness を強制ポリシー モードまたはモニタ モードで有効にするには、**ap namedot11airtime-fairness mode** コマンドを使用します。特定の AP の Air Time Fairness を 2 つのモードのいずれかから無効にするには、このコマンドの **no** 形式を使用します。

ap name*ap-name***dot11**{**24ghz**| **5ghz**} **airtime-fairness mode**{**enforce-policy**| **monitor**}

ap name*ap-name***nodot11**{**24ghz**| **5ghz**} **airtime-fairness mode**{**enforce-policy**| **monitor**}

構文の説明

ap-name	アクセス ポイント名を入力します。
24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
enforce-policy	強制ポリシー モードで Air Time Fairness を設定します。
monitor	モニタ モードで Air Time Fairness を設定します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、特定の AP の Air Time Fairness を強制ポリシー モードまたはモニタ モードのいずれかから無効にする例を示します。

```
Device# ap name testap no dot11 24ghz airtime-fairness mode
```

ap name dot11 airtime-fairness optimization

特定の AP の ATF 最適化を有効にするには、**ap name dot11airtime-fairness optimization** コマンドを使用します。特定の AP の ATF 最適化を無効にするには、**no** を使用します。

ap name*ap-name***dot11** {**24ghz**| **5ghz**} **airtime-fairness optimization**

ap name*ap-name***nodot11** {**24ghz**| **5ghz**} **airtime-fairness optimization**

構文の説明

ap-name	アクセス ポイント名を入力します。
24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、特定の AP の ATF 最適化を有効にする例を示します。

```
Device#ap name doctestap dot11 24ghz airtime-fairness optimization
```

ap name no dot11 airtime-fairness wlan-name policy-name

WLAN 固有の WLAN で ATF ポリシー オーバーライドを無効にするには、**ap name no dot11 airtime-fairness wlan-name** コマンドを使用します。

ap name*ap-name***no dot11**{**24ghz**| **5ghz**}**airtime-fairness wlan-name***wlan-name*

構文の説明

ap-name	アクセス ポイント名を入力します。
24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
wlan-name	シスコの AP でこの WLAN の Air Time Fairness ポリシーを設定します。
wlan-name	WLAN プロファイル名を入力します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、WLAN 固有の WLAN で ATF ポリシー オーバーライドを無効にする例を示します。

```
Device#ap name testap no dot11 24ghz airtime-fairness wlan-name testwlan
```

ap name dot11 airtime-fairness wlan-name policy

1 つの AP に固有の WLAN で ATF ポリシーをオーバーライドするには、**ap name dot11 airtime-fairness wlan-name policy-name** コマンドを使用します。

ap name*ap-name***dot11** {**24ghz**| **5ghz**} **airtime-fairnesswlan-name***wlan-name***policy-name***policy-name*

構文の説明

ap-name	アクセス ポイント名。
24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
wlan-name	シスコの AP でこの WLAN の Air Time Fairness ポリシーを設定します。
wlan-name	WLAN プロファイル名を入力します。
policy-name	Air Time Fairness ポリシーを設定します。
policy-name	Air Time Fairness ポリシー名を入力します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、1 つの AP に固有の WLAN で ATF ポリシーをオーバーライドする例を示します。

```
Device# ap name testap dot11 24ghz airtime-fairness wlan-name testwlan policy-name testpolicy
```

band-select client

選択した帯域のクライアントしきい値の最小 dB を設定するには、**band-select client** コマンドを使用します。選択した帯域のクライアントしきい値の最小dBをリセットするには、このコマンドの **no** 形式を使用します。

band-select client{**mid-rssi**| **rssi**}*dBm value*

構文の説明

mid-rssi	クライアント RSSI がプローブへの応答を開始するための最小 dBm。
rssi	クライアント RSSI がプローブへ応答するための最小 dBm。
dBm value	クライアント RSSI がプローブへ応答するための最小 dBm。有効な範囲は -90 ～ -20 dBm です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 2.4 GHz 帯域でのみ有効です。
次に、選択した帯域のクライアントしきい値を最小 dB に設定する例を示します。

```
Device(config-rf-profile)#band-select client rssi -50
```

band-select cycle

帯域選択のサイクル パラメータを設定するには、**band-select cycle** コマンドを使用します。しきい値をリセットするには、このコマンドの **no** 形式を使用します。

band-select cycle{ **count**|**threshold**} *value*

構文の説明

count	帯域選択のプローブ サイクル カウントを設定します。
value	応答していないサイクルの最大数。範囲は 1 ～ 10 です。
threshold	新規スキャン サイクルの時間しきい値を設定します。
value	しきい値をミリ秒単位で設定します。有効な値は、1 ～ 1000 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、選択した帯域の RF プロファイルにプローブ サイクル カウントを設定する例を示します。

```
Device(config-rf-profile)#band-select cycle count 5
```

band-select expire

選択した帯域の RF プロファイルの期限を設定するには、**band-select expire** コマンドを使用します。値をリセットするには、このコマンドの **no** 形式を使用します。

band-select expire{ **dual-band**| **suppression**}*value*

no band-select expire{ **dual-band**| **suppression**}

構文の説明

dual-band	RF プロファイルで帯域選択されたデュアル バンドの期限を設定します。
value	既知のデュアルバンドクライアントをプルーニングするための期限を設定します。範囲は 10 ～ 300 です。
suppression	RF プロファイルで帯域選択された抑制対象の期限を設定します。
value	既知の 802.11b/g クライアントをプルーニングするための期限を設定します。範囲は 10 ～ 200 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、選択した帯域の RF プロファイルのデュアルバンドに期限を設定する例を示します。

```
Device(config-rf-profile)#band-select expire dual-band 15
```

band-select probe-response

選択した帯域でのクライアントへのプローブ応答を設定するには、**band-select probe-response** コマンドを使用します。プローブ応答を無効にするには、このコマンドの **no** 形式を使用します。

band-select probe-response

構文の説明

probe-response	クライアントへのプローブ応答。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし
次に、クライアントへのプローブ応答を有効にする例を示します。

```
Device(config-rf-profile)#band-select probe-response
```

channel

RF プロファイルの DCA チャネル リストのチャネルを設定するには、**channel** コマンドを使用します。チャネルを無効にするには、このコマンドの **no** 形式を使用します。

channel{ **add**| **remove**} *channel-number*

構文の説明

add	RF プロファイルの DCA チャネル リストにチャネルを追加します。
remove	RF プロファイルの DCA チャネル リストからチャネルを削除します。
channel-number	チャネル番号。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの DCA チャネル リストにチャネルを追加する例を示します。

```
Device(config-rf-profile)#channel add 3
```

channel foreign

RF プロファイルの外部 AP の寄与を設定するには、**channel foreign** コマンドを使用します。DCA 外部 AP の寄与を無効にするには、このコマンドの **no** 形式を使用します。

channel foreign

構文の説明

foreign	RF プロファイルの DCA 外部 AP の寄与を設定します。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの DCA 外部 AP の寄与を設定する例を示します。

```
Device(config-rf-profile)#channel foreign
```

チャネル幅

RF プロファイルの DCA チャネル幅を設定するには、**channel width** 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。

チャネル幅{**20**| **40**| **80**| **best**}

構文の説明

20	MHz 単位のチャネル幅。
40	MHz 単位のチャネル幅。
80	MHz 単位のチャネル幅。
best	MHz 単位のチャネル幅。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 5 GHz 帯域でのみ有効です。
次に、チャネル幅を 40 MHzに設定する例を示します。

```
Device(config-rf-profile)#channel width 40
```

coverage

音声とデータの対象範囲を設定するには、**coverage** コマンドを使用します。最小RSSI値をリセットするには、このコマンドの **no** 形式を使用します。

coverage{**data**| **voice**} **rssi threshold***value*

構文の説明

data	データ パケットのカバレッジ ホール検出を設定します。
voice	音声パケットのカバレッジ ホール検出を設定します。
value	アクセスポイントが受信したパケットの最小RSSI値。有効な範囲は、-90 ～ -60 dBm です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし
次に、データ パケットのカバレッジ ホール検出を設定する例を示します。

```
Device(config-rf-profile)#coverage data rssi threshold -85
```

coverage exception

Cisco AP カバレッジ例外レベルを設定するには、**coverage exception** コマンドを使用します。例外レベルのパーセンテージをリセットするには、このコマンドの **no** 形式を使用します。

coverage exception*exception-level*

構文の説明

exception-level	有効な範囲が 0 ~ 100 % の Cisco AP カバレッジ例外レベル。

コマンド デフォルト

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、Cisco AP カバレッジ例外レベルを設定する例を示します。

```
Device(config-rf-profile)#coverage exception 70
```

coverage level

Cisco AP クライアントの最低のカバレッジ レベルを設定するには、**coverage level** コマンドを使用します。カバレッジクライアント値をリセットするには、このコマンドの **no** 形式を使用します。

coverage level *clients*

構文の説明

clients	最低のカバレッジ レベル。範囲は、1 ～ 200 クライアントです。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、Cisco AP クライアントの最低レベルを設定する例を示します。

```
Device(config-rf-profile)#coverage level 180
```

clear wireless airtime-fairness statistics

ワイヤレス通信時間フェアネス統計情報をクリアするには、**clear wireless airtime-fairness statistics** コマンドを使用します。

clearclear wireless airtime-fairness statistics

構文の説明

airtime-fairness	通信時間フェアネス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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、ワイヤレス通信時間フェアネス統計情報をクリアする例を示します。

```
Device#clear wireless airtime-fairness statistics
```

dot11n-only

RF プロファイルの 802.11n クライアント専用モードを有効にするには、**dot11n-only** コマンドを使用します。802.11n クライアント専用モードを無効にするには、このコマンドの **no** 形式を使用します。

dot11n-only

構文の説明

dot11n-only	RF プロファイルの 802.11n クライアント専用モード。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの 802.11n クライアント専用モードを有効にする例を示します。

```
Device(config-rf-profile)#dot11n-only
```

load-balancing

RF プロファイルのロード バランスを設定するには、**load-balancing** コマンドを使用します。RF プロファイルのロード バランス値をリセットするには、このコマンドの **no** 形式を使用します。

load-balancing{**denial**|**window**} *value*

構文の説明

denial	ロード バランシングの拒否の数を設定します。
value	ロード バランシングの拒否回数を入力します。範囲は 1 ～ 10 です。
window	アグレッシブ ロード バランシング用のクライアント ウィンドウを設定します。
value	クライアント数。範囲は 0 ～ 20 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、ロード バランシングの拒否の数を設定する例を示します。

```
Device#load-balancing denial 4
```

high-density clients count

RF プロファイルの最大クライアント数を設定するには、**high-density clients count** コマンドを使用します。RF プロファイルの最大クライアント数をリセットするには、このコマンドの **no** 形式を使用します。

high-density clients count*value*

構文の説明

value	AP 無線あたりの最大クライアント接続数。範囲は 0 ～ 200 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの最大クライアント数を設定する例を示します。

```
Device(config-rf-profile)#high-density clients count 25
```

high-density clients wlan

WLAN 上の AP あたりの最大クライアント数を設定するには、**high-density clients wlan** コマンドを使用します。最大数をリセットするには、このコマンドの **no** 形式を使用します。

high-density clients wlan *wlan name* **count** *count*

構文の説明

wlan name	AP あたりのクライアント数を制限するには、WLAN の名前を入力します。
count	WLAN ごとの AP あたりの最大クライアント接続数。範囲は 0 ～ 200 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、WLAN 上の AP あたりの最大クライアント数を設定する例を示します。

```
Device(config-rf-profile)#high-density clients wlan doctest count 20
```

high-density multicast data-rate

RF プロファイルのマルチキャスト データ レートの値を設定するには、 **high-density multicast data-rate** コマンドを使用します。データレートを auto 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。

high-density multicast data-rate{**RATE_12M| RATE_18M| RATE_24M| RATE_36M| RATE_48M| RATE_54M| RATE_6M| RATE_9M**}

構文の説明

multicast	RF プロファイルのマルチキャストを設定します。
data-rate	RF プロファイルのマルチキャスト データ レートの値。
RATE_12M	802.11 12M レート
RATE_18M	802.11 18M レート
RATE_24M	802.11 24M レート
RATE_36M	802.11 36M レート
RATE_48M	802.11 48M レート
RATE_54M	802.11 54M レート
RATE_6M	802.11 6M レート
RATE_9M	802.11 9M レート

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルのマルチキャスト データ レートの値を設定する例を示します。

```
Device(config-rf-profile)#high-density multicast data-rate RATE_9M
```

high-density rx-sop threshold

RF プロファイルの Rx SOPしきい値の値を設定するには、**high-density rx-sop threshold** コマンドを使用します。Rx SOP を auto に戻すには、このコマンドの **no** 形式を使用します。

high-density rx-sop threshold{**auto**| **high**| **low**| **medium**}

構文の説明

rx-sop	RF プロファイルの Rx SOP しきい値を設定します。
threshold	RF プロファイルの Rx SOP しきい値の値を設定します。
auto	無線レシーバ SOP しきい値を auto に戻します。
high	無線レシーバ SOP しきい値を high に設定します。
low	無線レシーバ SOP しきい値を low に設定します。
medium	無線レシーバ SOP しきい値を medium に設定します。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの無線レシーバ SOP しきい値を high に設定する例を示します。

```
Device(config-rf-profile)#high-density rx-sop threshold high
```

rate

802.11 動作速度を設定するには、**rate** コマンドを使用します。レート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。

rate{**RATE_12M**| **RATE_18M**| **RATE_24M**| **RATE_36M**| **RATE_48M**| **RATE_54M**| **RATE_6M**| **RATE_9M**}{**disable**| **mandatory**| **supported**}

構文の説明

RATE_12M	802.11 12M レート。
RATE_18M	802.11 18M レート。
RATE_24M	802.11 24M レート。
RATE_36M	802.11 36M レート。
RATE_48M	802.11 48M レート。
RATE_54M	802.11 54M レート。
RATE_6M	802.11 6M レート。
RATE_9M	802.11 9M レート。
disable	レートをディセーブルにします。
必須	レートを mandatory に設定します。
サポート	レートを supported に設定します。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、802.11 9M 動作速度を無効にする例を示します。

```
Device(config-rf-profile)#rate RATE_9M disable
```

rate mcs

RF プロファイルの MCS データ レートを有効にするには、**rate mcs** コマンドを使用します。RF プロファイルの MCS データ レートを無効にするには、このコマンドの **no** 形式を使用します。

rate mcs *index-number*

構文の説明

index-number	RF プロファイルの MCS データ レートのインデックス番号を入力します。範囲は 0 ～ 31 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの MCS データ レートを有効にする例を示します。

```
Device(config-rf-profile)#rate mcs 5
```

trap threshold

RF プロファイルのトラップしきい値パラメータを設定するには、**trap threshold** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文の説明

trap threshold {**clients**| **interference**| **noise**| **utilization**} *value*

clients	しきい値クライアントの RF プロファイル トラップを設定します。

value	トラップが送信された後に、アクセスポイントに関連付けるクライアントの数。範囲は 1 ～ 200 です。
interference	RF プロファイルの干渉のトラップしきい値を設定します。
value	RFプロファイルのトラップしきい値に干渉の割合値を設定します。範囲は 0 ～ 100 です。
noise	RF プロファイルのノイズのトラップしきい値を設定します。
value	RF プロファイルのトラップしきい値にノイズの値を dbm 単位で設定します。範囲は -127 ～ 0 です。
utilization	RF プロファイルの使用率のトラップしきい値を設定します。
value	RFプロファイルのトラップしきい値に使用率の割合値を設定します。範囲は 0 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、クライアントの RF プロファイルのしきい値トラップを設定する例を示します。

```
Device(config-rf-profile)#trap threshold clients 10
```

tx-power

Tx 電力レベルを設定するには、**tx-power** 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。

tx-power{**min**| **max**} *dBm value*

構文の説明

max	最大 Auto-RF 送信電力を設定します。
min	最小 Auto-RF 送信電力を設定します。
dBm value	dBm 単位で値を入力します。範囲は -10 ～ 30 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、Tx 電力レベルを min に設定する例を示します。

```
Device(config-rf-profile)#tx-power min -14
```

tx-power v1 threshold

伝送パワー コントロール（TPC）バージョン 1 のしきい値を設定するには、**tx-power v1 threshold** コマンドを使用します。デフォルトの dBm 値に戻すには、このコマンドの **no** 形式を使用します。

tx-power v1 threshold *dBm value*

構文の説明

dBm value	伝送パワー コントロール バージョン 1 のしきい値。範囲は -80 ～ -50 dBm です。

コマンド デフォルト

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、TPCv1 しきい値を –75 dBm に設定する例を示します。

```
Device#tx-power v1 threshold -75
```

no ap dot11 airtime-fairness policy-name

Air Time Fairness ポリシーを削除するには、**no ap dot11airtime-fairness policy-name** コマンドを使用します。

noap dot11 airtime-fairness policy-name*policy-name*

構文の説明

policy-name	Air Time Fairness ポリシー名を入力します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、Air Time Fairness ポリシーを削除する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device# no ap dot11 airtime-fairness policy-name testpol
```

remote-lan

AP グループにリモート LAN を設定するには、**remote-lan** コマンドを使用します。AP グループからリモート LAN を削除するには、このコマンドの **no** 形式を使用します。

remote-lan *name*

構文の説明

name	リモート LAN の名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし
次に、AP グループにリモート LAN を設定する例を示します。

```
Device(config-apgroup)#remote-lan rlantest
```

rf-profile dot11 24ghz

2.4 GHz 帯域の AP グループに RF プロファイルを割り当てるには、**rf-profile dot11 24ghz** コマンドを使用します。

rf-profile dot11 24ghz*name*

構文の説明

name	現在の AP グループに割り当てられる RF プロファイルの名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、2.4 GHz 帯域の AP グループに RF プロファイルを割り当てる例を示します。

```
Device(config-apgroup)#rf-profile dot11 24ghz doctest
```

rf-profile dot11 5ghz

5 GHz 帯域の AP グループに RF プロファイルを割り当てるには、**rf-profile dot11 5ghz** コマンドを使用します。

rf-profile dot11 5ghz*name*

構文の説明

name	現在の AP グループに割り当てられる RF プロファイルの名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、5GHz 帯域の AP グループに RF プロファイルを割り当てる例を示します。

```
Device(config-apgroup)#rf-profile dot11 24ghz doc5test
```

show ap airtime-fairness ap-group

特定の AP グループの ATF 設定を表示するには、**show ap airtime-fairness ap-group** コマンドを使用します。

show ap airtime-fairness ap-group*group-name*

構文の説明

group-name	AP グループ名を入力します

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、特定の AP グループの ATF 設定の例を示します。

```
Device#show ap airtime-fairness ap-group ?
Site Description:
Airtime-fairness 2.4GHz Mode:: Disable
Airtime-fairness 2.4GHz Optimization : n/a
Airtime-fairness 5GHz Mode:: Disable
Airtime-fairness 5GHz Optimization : n/a
```

```
WLAN ID   WLAN Name                          Interface            ATF Policy(2.4GHz)    ATF
 Policy(5GHz)
-------------------------------------------------------------------------------------------------
```

show ap airtime-fairness (ap)

特定の AP の ATF 設定を表示するには、**show ap airtime-fairness** コマンドを使用します。

showap name*ap-name***airtime-fairness**

構文の説明

ap-name	アクセス ポイント名を入力します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、特定の AP の ATF 設定を表示する例を示します。

```
Device# show ap name testap airtime-fairness
```

show ap airtime-fairness（無線別）

無線別の Air Time Fairness 設定がある AP リストを表示するには、**show ap airtime-fairness** コマンドを使用します。

show ap airtime-fairness

構文の説明

コマンド デフォルト

このコマンドには引数またはキーワードはありません。

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、無線別の Air Time Fairness がある AP リストを表示する例を示します。

```
Device#show ap airtime-fairness
```

show ap airtime-fairness policy（すべて）

すべての設定済みポリシーを表示するには、**show ap airtime-fairness policy** コマンドを使用します。

show ap airtime-fairness policy

構文の説明

policy	Air Time Fairness ポリシー情報を表示します。

コマンド デフォルト

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、設定済みのすべての Air Time Fairness ポリシーを表示する例を示します。

```
Device#show ap airtime-fairness policy
Policy ID   Policy Name          Weight
----------------------------------------
23           f                     10
12           asd                   10
13           pol                   10
50           meaw                  45
20           pocy                  10
0            Default               10
```

show ap airtime-fairness wlan

Air Time Fairness ポリシーが適用されている設定済み WLAN の完全なリストを表示するには、**show ap airtime-fairness wlan** コマンドを使用します。

show ap airtime-fairness wlan

構文の説明

wlan	すべての WLAN の Air Time Fairness 設定を表示します。

コマンド デフォルト

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、ATF ポリシーが適用されている設定済み WLAN の完全なリストを表示する例を示します。

```
Device#show ap airtime-fairness wlan

WLAN ID     Profile Name                        ATF Profile Name         Weight
-------------------------------------------------------------------------------
12          doctestlan                          Default                  10
```

show ap dot11 24ghz

2.4 GHz RRM パラメータを表示するには、**showapdot1124ghz** コマンドを使用します。

show ap dot11 24ghz {**ccx**| **channel**| **coverage**| **group**| **l2roam**| **logging**| **monitor**| **profile**| **receiver**| **summary**| **txpower**}

構文の説明

ccx	すべての Cisco AP に対して 802.11b CCX 情報を表示します。
channel	802.11b チャネル割り当ての設定および統計情報を表示します。
coverage	802.11b カバレッジの設定と統計情報を表示します。
group	802.11b グループ化の設定と統計情報を表示します。

l2roam	802.11b l2roam 情報を表示します。
logging	802.11b イベント ロギングの設定と統計情報を表示します。
monitor	802.11b モニタリングの設定および統計情報を表示します。
profile	すべての Cisco AP の 802.11b プロファイル情報を表示します。
receiver	802.11b レシーバの設定と統計情報を表示します。
summary	802.11b Cisco AP の設定と統計情報を表示します。
txpower	802.11b 送信電力制御の設定と統計情報を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、802.11b カバレッジの設定と統計情報を表示する例を示します。

```
Device#show ap dot11 24ghz coverage

Coverage Hole Detection
  802.11b Coverage Hole Detection Mode            : Enabled
  802.11b Coverage Voice Packet Count             : 100 packet(s)
  802.11b Coverage Voice Packet Percentage        : 50%
  802.11b Coverage Voice RSSI Threshold           : -80 dBm
  802.11b Coverage Data Packet Count              : 50 packet(s)
  802.11b Coverage Data Packet Percentage         : 50%
  802.11b Coverage Data RSSI Threshold            : -80 dBm
  802.11b Global coverage exception level         : 25 %
  802.11b Global client minimum exception level   : 3 clients
```

show ap dot11 5ghz

5 GHz RRM パラメータを表示するには、**showapdot115ghz** コマンドを使用します。

show ap dot11 5ghz {**ccx**| **channel**| **coverage**| **group**| **l2roam**| **logging**| **monitor**| **profile**| **receiver**| **summary**| **txpower**}

構文の説明

ccx	すべての Cisco AP の 802.11a CCX 情報を表示します。
channel	802.11a チャネル割り当ての設定および統計情報を表示します。
coverage	802.11a カバレッジの設定と統計情報を表示します。
group	802.11a グループ化の設定と統計情報を表示します。
l2roam	802.11a l2roam 情報を表示します。
logging	802.11a イベント ロギングの設定と統計情報を表示します。
monitor	802.11a モニタリングの設定および統計情報を表示します。
profile	すべての Cisco AP の 802.11a プロファイル情報を表示します。
receiver	802.11a レシーバの設定と統計情報を表示します。
summary	802.11a Cisco AP の設定と統計情報を表示します。
txpower	802.11a 送信電力制御の設定と統計情報を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、802.11a チャネル割り当ての設定と統計情報の例を示します。

```
Device#show ap dot11 5ghz channel

Automatic Channel Assignment
  Channel Assignment Mode                       : AUTO
  Channel Update Interval                       : 12 Hours
  Anchor time (Hour of the day)                 : 20
  Channel Update Contribution                   : SNI..
  Channel Assignment Leader                     : web (9.9.9.2)
  Last Run                                      : 16534 seconds ago
  DCA Sensitivity Level                         : MEDIUM (15 dB)
  DCA 802.11n Channel Width                     : 40 Mhz
  Channel Energy Levels
      Minimum                                   : unknown
      Average                                   : unknown
      Maximum                                   : unknown
  Channel Dwell Times
      Minimum                                   : unknown
      Average                                   : unknown
      Maximum                                   : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                          : 36,40,44,48,52,56,60,64,149,153,1

                 57,161
  Unused Channel List                           : 100,104,108,112,116,132,136,140,1

                 65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                          :
  Unused Channel List                           : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,

                 15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                         : Disabled
```

show ap dot11 airtime-fairness（無線帯域）

ATF が設定された無線帯域がある AP リストを表示するには、**show ap dot11 airtime-fairness** コマンドを使用します。

showapdot11{24ghz| 5ghz}airtime-fairness

構文の説明

24ghz	802.11b の設定を表示します。
5ghz	802.11a の設定を表示します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、ATF が設定された無線帯域がある AP リストを表示する例を示します。

```
Device#show ap dot 24ghz airtime-fairness
```

show ap dot11 24ghz rf-profile summary

2.4 GHz RF プロファイルのサマリーを表示するには、**show ap dot11 24ghz rf-profile summary** コマンドを使用します。

show ap dot11 24ghz rf-profile summary

構文の説明

summary	RF プロファイルのサマリーを表示します。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に 24 GHz AP プロファイルのサマリーを表示する例を示します。

```
Device(config-rf-profile)#show ap dot11 24ghz rf-profile summaryNumber of RF Profiles : 1

RF Profile Name                  Band      Description           Applied   State
------------------------------------------------------------------------------
doctest                          2.4 GHz                         No        Down
```

show ap dot11 5ghz rf-profile summary

5 GHz AP の RF プロファイルを表示するには、**show ap dot11 5ghz rf-profile summary** コマンドを使用します。

show ap dot11 5ghz rf-profile summary

構文の説明

summary	RF プロファイルのサマリーを表示します。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、5 GHz AP の RF プロファイルのサマリーを表示する例を示します。

```
Device#show ap dot11 5ghz rf-profile summary
Number of RF Profiles : 1

RF Profile Name                  Band      Description           Applied   State
------------------------------------------------------------------------------
doc5test                         5 GHz                           No        Down
```

show ap name dot11 airtime-fairness summary

特定の AP の ATF 統計を表示するには、**show ap name dot11 airtime-fairness summary** コマンドを使用します。

showap name*ap-name***dot11**{**24ghz**| **5ghz**} **airtime-fairness summary**

構文の説明

ap-name	24 GHz と 5 GHz の Air Time Fairness の統計を表示します。
24ghz	802.11b の設定を表示します。
5ghz	802.11a の設定を表示します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、特定の AP の ATF 統計を表示する例を示します。

```
Device#show ap ame testap dot11 24ghz airtime-fairness summary
```

show ap name dot11 airtime-fairness policy statistics

各 ATF ポリシーの統計を表示するには、**show ap name dot11 airtime-fairness policy statistics** コマンドを使用します。

構文の説明

~~**showap name***ap-name***dot11**{**24ghz**| **5hz**} **airtime-fairness policy***policy-name***statistics**~~

ap-name	アクセス ポイント名を入力します。

24ghz	802.11b の設定を表示します。
5hz	802.11a の設定を表示します。
policy-name	ポリシー名を入力します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、各 ATF ポリシーの統計を表示する例を示します。

```
Device#show ap name testap dot11 24ghz airtime-fairness policy testpolicy statistics
```

show ap name dot11 airtime-fairness wlan name statistics

特定の AP でアクティブな WLAN ごとの ATF の統計を表示するには、**show ap name dot11 airtime-fairness wlan name statistics** コマンドを使用します。

showap namedot11 {**24ghz**| **5ghz**} **airtime-fairness wlan name***wlan-name***statistics**

構文の説明

name	プロファイル名別の Air Time Fairness の統計を表示します。
wlan-name	WLAN 名を入力します。
statistics	24 GHz と 5 GHz の Air Time Fairness の統計を表示します。

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
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、特定の AP でアクティブな WLAN ごとの ATF の統計を表示する例を示します。

```
Device#show ap name testap dot11 24ghz airtime-fairness wlan name testwlan statistics
```

show ap rf-profile summary

AP の RF プロファイルのサマリーを表示するには、**show ap rf-profile summary** コマンドを使用します。

show ap rf-profile summary

構文の説明

summary	RF プロファイルのサマリーを表示します。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP の RF プロファイルのサマリーを表示する例を示します。

```
Device#show ap rf-profile summary
Number of RF Profiles : 1

RF Profile Name                  Band      Description           Applied   State
------------------------------------------------------------------------------
```

```
doctest                          2.4 GHz                          No        Down
```

show ap rf-profile name

選択した AP の RF プロファイルの詳細を表示するには、**show ap rf-profile name** コマンドを使用します。

show ap rf-profile name*profile-name***detail**

構文の説明

profile-name	RF プロファイルの名前。
detail	選択した RF プロファイルの詳細を表示します。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、選択した RF プロファイルの詳細を表示する例を示します。

```
Device#show ap rf-profile name doctest detail
Description :
AP Group Names :
RF Profile Name : doctest
Band : 2.4 GHz
802.11n client only : Disabled
Transmit Power Threshold v1: -70 dBm
Min Transmit Power: -10 dBm
Max Transmit Power: 30 dBm
Operational Rates
  802.11b 1M Rate : Mandatory
  802.11b 2M Rate : Mandatory
  802.11b 5.5M Rate : Mandatory
  802.11b 11M Rate : Mandatory
  802.11b 6M Rate : Mandatory
  802.11b 9M Rate : Supported
```

```
  802.11b 12M Rate : Supported
  802.11b 18M Rate : Supported
  802.11b 24M Rate : Supported
  802.11b 36M Rate : Supported
  802.11b 48M Rate : Supported
  802.11b 54M Rate : Supported
Max Clients : 200
Wlan name                          Max Clients
-----------------------------------------

Trap Threshold
  Clients:  12 clients
  Interference:  10%
  Noise:  -70 dBm
  Utilization:  80%
Multicast Data Rate: auto
Rx SOP Threshold : auto
Band Select
  Probe Response:  Disabled
  Cycle Count:  2 cycles
  Cycle Threshold:  200 milliseconds
  Expire Suppression:  20 seconds
  Expire Dual Band:  60 seconds
  Client RSSI:  -80 dBm
  Client Mid RSSI:  -80 dBm
Load Balancing
  Window:  5 clients
  Denial:  3 count
Coverage Data
  Data: -80 dBm
  Voice: -80 dBm
 Minimum Client Level: 3 clients
  Exception Level: 25%
DCA Channel List  : 1,5,9,13
DCA Foreign AP Contribution : Enabled
802.11n MCS Rates
  MCS 0 : Enabled
  MCS 1 : Enabled
  MCS 2 : Enabled
  MCS 3 : Enabled
  MCS 4 : Enabled
  MCS 5 : Enabled
  MCS 6 : Enabled
  MCS 7 : Enabled
  MCS 8 : Enabled
  MCS 9 : Enabled
  MCS 10 : Enabled
  MCS 11 : Enabled
  MCS 12 : Enabled
  MCS 13 : Enabled
  MCS 14 : Enabled
  MCS 15 : Enabled
  MCS 16 : Enabled
  MCS 17 : Enabled
  MCS 18 : Enabled
  MCS 19 : Enabled
  MCS 20 : Enabled
  MCS 21 : Enabled
  MCS 22 : Enabled
  MCS 23 : Enabled
  MCS 24 : Enabled
  MCS 25 : Enabled
  MCS 26 : Enabled
  MCS 27 : Enabled
  MCS 28 : Enabled
  MCS 29 : Enabled
  MCS 30 : Enabled
  MCS 31 : Enabled
State : Down
```

show wireless mobility controller ap

サブドメインに参加したアクセスポイントの一覧を表示するには、**wireless mobility controller ap** コマンドを使用します。

show wireless mobility controller ap

構文の説明

ap	サブドメインに参加したアクセスポイントを表示します。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、サブドメインに参加したアクセスポイントを一覧する例を示します。

```
Device#show wireless mobility controller ap
Number of AP entries in the sub-domain     : 2

AP name                          AP radio MAC      Controller IP     Location
-------------------------------------------------------------------------------------------
bos2kk                           00f2.8c42.f520    default-group     default-group
IosAP1                           34ed.522f.7e60    default-group     default-group
```

シャットダウン

RF プロファイルを閉じて、ネットワークを無効にするには、**shutdown** コマンドを使用します。シャットダウンの実行を無効にするには、このコマンドの **no** 形式を使用します。

構文の説明

シャットダウン	プロファイルをシャットダウンし、ネットワークを無効にします。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルを閉じて、ネットワークを無効にする例を示します。

```
Device(config-rf-profile)#shutdown
```

wlan

AP グループに WLAN を設定するには、**wlan** コマンドを使用します。AP グループから VLAN を削除するには、このコマンドの **no** 形式を使用します。

wlan *wlan-name*

構文の説明

wlan-name	AP グループに設定される WLAN の名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP グループに VLAN を設定する例を示します。

```
Device(config-apgroup)#wlan docwlan
```

第 XVI 部

Routing

- 双方向フォワーディング検出コマンド，995 ページ

第 17 章

双方向フォワーディング検出コマンド

- authentication（BFD）, 995 ページ
- bfd, 996 ページ
- bfd all-interfaces, 998 ページ
- bfd check-ctrl-plane-failure, 999 ページ
- bfd echo, 1000 ページ
- bfd slow-timers, 1002 ページ
- bfd template, 1003 ページ
- bfd-template, 1004 ページ
- ip route static bfd, 1005 ページ
- ipv6 route static bfd, 1007 ページ

authentication（BFD）

シングルホップ セッション用の Bidirectional Forwarding Detection（BFD）テンプレートで認証を設定するには、BFD コンフィギュレーション モードで **authentication** コマンドを使用します。シングルホップ セッション用の BFD テンプレートで認証を無効にするには、このコマンドの **no** 形式を使用します。

authentication *authentication-type* **keychain** *keychain-name*

no authentication *authentication-type* **keychain** *keychain-name*

構文の説明

authentication-type	認証タイプ。有効な値は、md5、meticulous-md5、meticulous-sha1、および sha-1 です。

keychain*keychain-name*	指定された名前で認証キーチェーンを設定します。この名前の長さは最大 32 文字です。

コマンド デフォルト

シングルホップ セッション用の BFD テンプレートでは認証が有効になっていません。

コマンド モード

BFD コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

シングルホップ テンプレートで認証を設定できます。セキュリティを強化するために認証を設定することをお勧めします。認証は、BFD の送信元と宛先のペアごとに設定する必要があり、認証パラメータは両方のデバイスで同じである必要があります。

次に、BFD シングルホップ テンプレートの template1 で認証を設定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# bfd-template single-hop template1
デバイス(config-bfd)# authentication sha-1 keychain bfd-singlehop
```

bfd

インターフェイスに対してベースライン Bidirectional Forwarding Detection（BFD）セッション 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 **bfd** コマンドを使用します。ベースライン BFD セッション 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。

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

構文の説明

interval *milliseconds*	BFD 制御パケットが BFD ピアに送信される速度（ミリ秒単位）を指定します。milliseconds 引数の有効範囲は 50 ～ 9999 です。

min_rx *milliseconds*	BFD 制御パケットが BFD ピアで受信されるものと期待される速度（ミリ秒単位）を指定します。milliseconds 引数の有効範囲は 50 ～ 9999 です。
multiplier *multiplier-value*	BFD ピアから連続して紛失してよい BFD 制御パケットの数を指定します。この数に達すると、BFDはそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。multiplier-value 引数の有効範囲は 3 ～ 50 です。

コマンド デフォルト

ベースライン BFD セッション パラメータの設定はありません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

bfd コマンドは、SVI、イーサネット、およびポートチャネルインターフェイスで設定できます。

BFD がポート チャネル インターフェイスで実行されている場合は、BFD には、250 * 3 ミリ秒のタイマー値制限があります。

bfd interval 設定は次のような場合には削除されません。

- IPv4 アドレスがインターフェイスから削除された場合
- IPv6 アドレスがインターフェイスから削除された場合
- IPv6 がインターフェイスからディセーブルにされた場合
- インターフェイスがシャットダウンされた場合
- インターフェイスで IPv4 CEF がグローバルまたはローカルでディセーブルにされた場合
- インターフェイスで IPv6 CEF がグローバルまたはローカルでディセーブルにされた場合

bfd interval 設定は、それを設定したサブインターフェイスが削除されたときに削除されます。

（注） インターフェイス コンフィギュレーション モードで bfd interval コマンドを設定すると、デフォルトで BFD エコー モードが有効になります。インターフェイス コンフィギュレーション モードで no ip redirect（BFD エコーが必要な場合）または no bfd echo のいずれかを有効にする必要があります。

CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、no ip redirect コマンドを入力して、インターネット制御メッセージプロトコル（ICMP）リダイレクト メッセージの送信を無効にする必要があります。

次に、ギガビット イーサネット 1/0/3 の BFD セッション パラメータを設定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# interface gigabitethernet 1/0/3
デバイス(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

bfd all-interfaces

ルーティング プロセスに参加しているすべてのインターフェイスの Bidirectional Forwarding Detection（BFD）を有効にするには、ルータ コンフィギュレーション モードまたはアドレス ファミリ インターフェイス コンフィギュレーション モードで **bfd all-interfaces** コマンドを使用します。1 つのインターフェイスですべてのネイバーの BFD を無効にするには、このコマンドの **no** 形式を使用します。

bfd all-interfaces

no bfd all-interfaces

構文の説明

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

ルーティング プロセスに参加しているインターフェイスの BFD が無効になっています。

コマンド モード

ルータ コンフィギュレーション（config-router）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

すべてのインターフェイスの BFD を有効にするには、ルータ コンフィギュレーション モードで bfd all-interfaces コマンドを入力します。

次に、すべての Enhanced Interior Gateway Routing Protocol（EIGRP）ネイバーの BFD を有効にする例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# router eigrp 123
デバイス(config-router)# bfd all-interfaces
デバイス(config-router)# end
```

次に、すべての Intermediate System-to-Intermediate System（IS-IS）ネイバーの BFD を有効にする例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# router isis tag1
デバイス(config-router)# bfd all-interfaces
デバイス(config-router)# end
```

bfd check-ctrl-plane-failure

Intermediate System-to-Intermediate System（IS-IS）ルーティング プロトコルの Bidirectional Forwarding Detection（BFD）コントロール プレーン障害チェックを有効にするには、ルータ コンフィギュレーション モードで **bfd check-control-plane-failure** コマンドを使用します。コントロール プレーン障害検出を無効にするには、このコマンドの **no** 形式を使用します。

bfd check-ctrl-plane-failure

no bfd check-ctrl-plane-failure

構文の説明

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

BFD コントロール プレーン障害チェックが無効になっています。

コマンド モード

ルータ コンフィギュレーション（config-router）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

bfd check-ctrl-plane-failure コマンドは、IS-IS ルーティング プロセスについてのみ設定できます。このコマンドは、他のプロトコルではサポートされていません。

スイッチが再起動すると、見せかけの BFD セッション障害が発生する場合があります。このとき、隣接ルータは、転送障害が本当に発生したかのように動作します。ただし、スイッチで bfd check-control-plane-failure コマンドが有効になっていると、ルータはコントロールプレーン関連の BFD セッション障害を無視できます。ルータを再起動する予定がある場合は、直前にすべての隣接ルータの設定にこのコマンドを追加し、再起動が完了したときにすべての隣接ルータからこのコマンドを削除することをお勧めします。

次に、IS-IS ルーティング プロトコルの BFD コントロール プレーン障害チェックを有効にする例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# router isis
デバイス(config-router)# bfd check-ctrl-plane-failure
デバイス(config-router)# end
```

bfd echo

Bidirectional Forwarding Detection（BFD）エコー モードを有効にするには、インターフェイス コンフィギュレーション モードで **bfd echo** コマンドを使用します。BFD エコー モードを無効にするには、このコマンドの **no** 形式を使用します。

bfd echo

no bfd echo

構文の説明

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 コンフィギュレーション モードで bfd interval コマンドを使用して BFD を設定している場合は、BFD エコー モードがデフォルトで有効になります。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

エコー モードはデフォルトでイネーブルになっています。キーワードを指定せずに **no bfd echo** コマンドを入力すると、エコー パケットの送信がオフになり、スイッチが BFD ネイバー スイッチから受信したエコー パケットを転送しないことを示します。

エコー モードを有効にすると、必要最短エコー送信間隔と必要最短送信間隔の値が **bfd interval***milliseconds***min_rx***milliseconds* パラメータから取得されます。

（注） CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、**no ip redirects** コマンドを入力して、インターネット制御メッセージプロトコル（ICMP）リダイレクトメッセージの送信を無効にする必要があります。

次に、BFD ネイバー間でエコー モードを設定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# interface GigabitEthernet 1/0/3
デバイス(config-if)# bfd echo
```

show bfd neighbors details コマンドの次の出力は、BFD セッション ネイバーが BFD エコー モードで稼働しているところを示します。この出力では、対応するコマンド出力が太字で表示されています。

```
デバイス# show bfd neighbors details
OurAddr      NeighAddr   LD/RD  RH/RS  Holdown(mult) State Int
172.16.1.2   172.16.1.1  1/6    Up     0 (3 )        Up    Fa0/1
Session state is UP and using echo function with 100 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000   - Min rx interval: 1000000
             Min Echo interval: 50000
```

bfd slow-timers

Bidirectional Forwarding Detection（BFD） スロー タイマー値を設定するには、インターフェイス コンフィギュレーション モードで **bfd slow-timers** コマンドを使用します。BFD によって使用されるスロー タイマーを変更するには、このコマンドの **no** 形式を使用します。

bfd slow-timers [*milliseconds*]

no bfd slow-timers

コマンド デフォルト

BFD スロー タイマー値は 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、BFD スロー タイマー値を 14,000 ミリ秒に設定する例を示します。

```
デバイス(config)# bfd slow-timers 14000
```

show bfd neighbors details コマンドの次の出力は、BFD スロー タイマー値 14,000 ミリ秒が実装されているところを示します。MinTxInt および MinRxInt の値は BFD スロー タイマーの設定値に対応しています。関連するコマンド出力は太字で示されています。

```
デバイス# show bfd neighbors details
OurAddr      NeighAddr   LD/RD  RH/RS  Holdown(mult) State Int
172.16.1.2   172.16.1.1  1/6    Up     0 (3 )        Up    Fa0/1
Session state is UP and using echo function with 100 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 14000, MinRxInt: 14000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3600(0), Hello (hits): 1200(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000   - Min rx interval: 1000000
             Min Echo interval: 50000
```

（注）
- BFD セッションがダウンすると、BFD 制御パケットがスロー タイマー間隔で送信されます。
- BFD セッションが稼働している場合、エコーが有効になっていれば、BFD 制御パケットがネゴシエートされたスロー タイマー間隔で送信され、エコー パケットがネゴシエートされた設定済みの BFD 間隔で送信されます。エコーが有効になっていない場合は、BFD 制御パケットがネゴシエートされた設定済みの間隔で送信されます。

bfd template

シングルホップ Bidirectional Forwarding Detection（BFD）テンプレートをインターフェイスにバインドするには、インターフェイス コンフィギュレーション モードで **bfd template** コマンドを使用します。シングルホップ BFD テンプレートをインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

bfd template *template-name*

no bfd template *template-name*

コマンド デフォルト

BFD テンプレートはインターフェイスにバインドされません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

bfd-template コマンドを使用してテンプレートを作成していない場合でも、インターフェイスでテンプレート名を設定できますが、テンプレートを定義するまでテンプレートは無効と見なされます。テンプレート名を再設定する必要はありません。名前は自動的に有効になります。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# interface Gigabitethernet 1/3/0
デバイス(config-if)# bfd template template1
```

bfd-template

Bidirectional Forwarding Detection（BFD）テンプレートを設定し、BFD 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 **bfd-template** コマンドを使用します。BFD テンプレ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。

bfd-template single-hop *template-name*

no bfd-template single-hop *template-name*

構文の説明

single-hop	シングルホップ BFD テンプレートを作成します。
template-name	テンプレート名。

コマンド デフォルト

BFD テンプレートは存在しません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

bfd template コマンドを使用すると BFD テンプレートを作成し、デバイスを BFD コンフィギュレーション モードにすることができます。テンプレートは一連の BFD 間隔値を指定するために使用できます。BFD テンプレートの一部として指定される BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。

次に、BFD テンプレートを作成し、BFD 間隔値を指定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# bfd-template single-hop node1
デバイス(bfd-config)#interval min-tx 100 min-rx 100 multiplier 3
デバイス(bfd-config)#echo
```

次に、BFD シングルホップ テンプレートを作成し、BFD 間隔値と認証キー チェーンを設定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# bfd-template single-hop template1
デバイス(bfd-config)#interval min-tx 200 min-rx 200 multiplier 3
デバイス(bfd-config)#authentication keyed-sha-1 keychain bfd_singlehop
```

（注） デフォルトでは、BFD テンプレート設定で BFD エコーは有効になっていません。これは明示的に設定する必要があります。

ip route static bfd

スタティック ルートの双方向フォワーディング検出（BFD）ネイバーを指定するには、グローバル コンフィギュレーション モードで **ip route static bfd** コマンドを使用します。スタティック ルートの BFD ネイバーを削除するには、このコマンドの **no** 形式を使用します。

ip route static bfd {*interface-type interface-number ip-address* | **vrf***vrf-name*} [**group***group-name*] **[passive] [unassociate]**

no ip route static bfd {*interface-type interface-number ip-address* | **vrf***vrf-name*} [**group***group-name*] **[passive] [unassociate]**

構文の説明

interface-type interface-number	インターフェイスのタイプと番号
ip-address	A.B.C.D 形式のゲートウェイの IP アドレス。
vrf*vrf-name*	Virtual Routing and Forwarding（VRF）インスタンスと宛先の vrf 名を指定します。
group*group-name*	（任意）BFD グループを割り当てます。group-name は BFD グループ名を指定する最大 32 文字の文字列です。
unassociate	（任意）BFD に設定されたスタティック ルートの関連付けを解除します。

コマンド デフォルト

グローバル ルート BFD ネイバーは指定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 ルート BFD ネイバーを指定するには、ip route static bfd コマンドを使用します。設定に指定されている同一のインターフェイスとゲートウェイを保持するスタティック ルートはすべて、到達可能性通知を得るために同一の BFD セッションを共有します。

interface-type interface-number および ip-address 引数に同じ値が指定されているスタティック ルートはすべて、自動的に BFD を使用して、ゲートウェイの到達可能性を判別し、高速障害検出を利用します。

group キーワードは BFD グループを割り当てます。スタティック BFD 設定は、インターフェイスが関連付けられている VPN ルーティングおよび転送（VRF）インスタンスに追加されます。**passive** キーワードは、グループのパッシブ メンバーを指定します。passive キーワードなしでグループにスタティック BFD を追加すると、BFD がグループのアクティブ メンバーになります。グループの BFD セッションをトリガーするために、スタティック ルートをアクティブ BFD 設定によって追跡する必要があります。特定のグループのすべてのスタティック BFD 設定（アクティブとパッシブ）を削除するには、**no ip route static bfd** コマンドを使用して、BFD グループ名を指定します。

unassociate キーワードは、BFD ネイバーがスタティック ルートに関連付けられることなく、インターフェイスに BFD が設定されている場合に BFD セッションが要求されることを指定します。これは IPv4 スタティック ルートがない BFDv4 セッションを起動するために役立ちます。unassociate キーワードを指定しない場合は、IPv4 スタティック ルートが BFD セッションに関連付けられます。

BFD では、両方のエンドポイント デバイス BFD セッションが開始されている必要があります。そのため、このコマンドは各エンドポイント デバイスで設定する必要があります。

スイッチ仮想インターフェイス（SVI）の BFD スタティック セッションは、その SVI 上で無効だった **bfd interval***milliseconds***min_rx***milliseconds***multiplier***multiplier-value* コマンドが有効化された後にのみ確立されます。

スタティック BFD セッションを有効にするには、次の手順を実行します。

1. SVI で BFD タイマーを有効にします。

   bfd interval*milliseconds***min_rx***milliseconds***multiplier***multiplier-value*

2. スタティック IP ルートの BFD を有効にします。

   ip route static bfd*interface-type interface-number ip-address*

3. SVI で BFD タイマーを無効にし、再度有効にします。

   no bfd interval*milliseconds***min_rx***milliseconds***multiplier***multiplier-value*

bfd interval*milliseconds***min_rx***milliseconds***multiplier***multiplier-value*

次に、指定したネイバー、グループおよびグループのアクティブ メンバーを介してすべてのスタティック ルートの BFD を設定する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ip route static bfd GigabitEthernet 1/0/1 10.1.1.1 group group1
```

次に、指定したネイバー、グループおよびグループのパッシブ メンバーを介してすべてのスタティック ルートの BFD を設定する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 group group1 passive
```

次に、group および passive キーワードを指定せず、無関係なモードですべてのスタティック ルートの BFD を設定する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 unassociate
```

ipv6 route static bfd

IPv6（BFDv6）ネイバーのためのスタティック ルートの双方向フォワーディング検出を指定するには、グローバル コンフィギュレーション モードで **ipv6 route static bfd** コマンドを使用します。スタティック ルートの BFDv6 ネイバーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 route static bfd [**vrf***vrf-name*] *interface-type interface-number ipv6-address* **[unassociated]**

no ipv6 route static bfd

構文の説明

vrf*vrf-name*	（任意）スタティック ルートを指定する必要がある Virtual Routing and Forwarding（VRF）インスタンスの名前。
interface-type interface-number	インターフェイスのタイプと番号
ipv6-address	ネイバーの IPv6 アドレス。
unassociated	（任意）スタティック BFD ネイバーを関連付けられたモードから無関係なモードに移行します。

コマンド デフォルト

スタティック ルートの BFDv6 ネイバーは指定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 ルートのネイバーを指定するには、ipv6 route static bfd コマンドを使用します。設定に指定されている同一のインターフェイスとゲートウェイを保持するスタティック ルートはすべて、到達可能性通知を得るために同一の BFDv6 セッションを共有します。BFDv6 では、両方のエンドポイントのルータで BFDv6 セッションが開始されている必要があります。そのため、このコマンドは各エンドポイント ルータで設定する必要があります。IPv6 スタティック BFDv6 ネイバーは、インターフェイスとネイバー アドレスで完全に指定される必要があり、直接接続されている必要があります。

vrf vrf-name、interface-type interface-number および *ipv6-address* に同じ値が指定されているスタティック ルートはすべて、自動的に BFDv6 を使用して、ゲートウェイの到達可能性を判別し、高速障害検出を利用します。

次に、アドレスが 2001::1 のイーサネット インターフェイス 0/0 でネイバーを作成する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ipv6 route static bfd ethernet 0/0 2001::1
```

次に、ネイバーを無関係なモードに変換する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```

第 XVII 部

セキュリティ

- セキュリティ コマンド，1011 ページ

第 18 章

セキュリティ コマンド

- aaa accounting dot1x, 1014 ページ
- aaa accounting identity, 1016 ページ
- aaa authentication dot1x, 1018 ページ
- aaa authorization, 1019 ページ
- aaa new-model, 1024 ページ
- access-session mac-move deny, 1026 ページ
- action, 1027 ページ
- authentication host-mode, 1029 ページ
- authentication mac-move permit, 1030 ページ
- 認証優先, 1032 ページ
- authentication violation, 1035 ページ
- cisp enable, 1036 ページ
- clear errdisable interface vlan, 1038 ページ
- clear mac address-table, 1039 ページ
- cts manual, 1041 ページ
- cts role-based enforcement, 1042 ページ
- cts role-based l2-vrf, 1044 ページ
- cts role-based monitor, 1046 ページ
- cts role-based permissions, 1047 ページ
- deny（MAC アクセス リスト コンフィギュレーション）, 1049 ページ
- device-role（IPv6 スヌーピング）, 1052 ページ

- device-role（IPv6 ND 検査）, 1053 ページ
- device-tracking policy, 1055 ページ
- dot1x critical（グローバル コンフィギュレーション）, 1056 ページ
- dot1x max-start, 1057 ページ
- dot1x pae, 1058 ページ
- dot1x supplicant controlled transient, 1059 ページ
- dot1x supplicant force-multicast, 1060 ページ
- dot1x test eapol-capable, 1062 ページ
- dot1x test timeout, 1063 ページ
- dot1x timeout, 1064 ページ
- epm access-control open, 1066 ページ
- ip access-list role-based, 1068 ページ
- ip admission, 1069 ページ
- ip admission name, 1070 ページ
- ip device tracking maximum, 1072 ページ
- ip device tracking probe, 1074 ページ
- ip dhcp snooping database, 1075 ページ
- ip dhcp snooping information option format remote-id, 1077 ページ
- ip dhcp snooping verify no-relay-agent-address, 1078 ページ
- ip http access-class, 1079 ページ
- ip source binding, 1081 ページ
- ip verify source, 1082 ページ
- ipv6 access-list, 1084 ページ
- ipv6 snooping policy, 1086 ページ
- key chain macsec, 1087 ページ
- limit address-count, 1089 ページ
- mab request format attribute 32, 1090 ページ
- macsec network-link, 1092 ページ
- match（アクセス マップ コンフィギュレーション）, 1092 ページ
- mka pre-shared-key, 1094 ページ
- no authentication logging verbose, 1095 ページ

- no dot1x logging verbose, 1096 ページ
- no mab logging verbose, 1097 ページ
- permit（MAC アクセス リスト コンフィギュレーション）, 1098 ページ
- propagate sgt (cts manual), 1102 ページ
- protocol（IPv6 スヌーピング）, 1104 ページ
- sap mode-list (cts manual), 1105 ページ
- security level（IPv6 スヌーピング）, 1107 ページ
- security passthru, 1108 ページ
- show aaa clients, 1109 ページ
- show aaa command handler, 1109 ページ
- show aaa local, 1110 ページ
- show aaa servers, 1111 ページ
- show aaa sessions, 1112 ページ
- show authentication history, 1113 ページ
- show authentication sessions, 1114 ページ
- show cts interface, 1116 ページ
- show cts role-based permissions, 1119 ページ
- show cisp, 1121 ページ
- show dot1x, 1122 ページ
- show eap pac peer, 1124 ページ
- show ip dhcp snooping statistics, 1124 ページ
- show radius server-group, 1127 ページ
- show storm-control, 1129 ページ
- show vlan access-map, 1131 ページ
- show vlan filter, 1132 ページ
- show vlan group, 1133 ページ
- storm-control, 1134 ページ
- switchport port-security aging, 1137 ページ
- switchport port-security mac-address, 1139 ページ
- switchport port-security maximum, 1142 ページ
- switchport port-security violation, 1144 ページ

- tracking（IPv6 スヌーピング），1146 ページ
- trusted-port，1148 ページ
- wireless dot11-padding，1149 ページ
- wireless security dot1x，1150 ページ
- wireless security lsc，1152 ページ
- wireless security strong-password，1153 ページ
- wireless wps ap-authentication，1154 ページ
- wireless wps auto-immune，1155 ページ
- wireless wps cids-sensor，1156 ページ
- wireless wps client-exclusion，1157 ページ
- wireless wps mfp infrastructure，1158 ページ
- wireless wps rogue，1159 ページ
- wireless wps shun-list re-sync，1160 ページ
- vlan access-map，1161 ページ
- vlan filter，1163 ページ
- vlan group，1164 ページ

aaa accounting dot1x

認証、認可、およびアカウンティング（AAA）アカウンティングをイネーブルにして、IEEE 802.1x セッションの特定のアカウンティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。IEEE 802.1x アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

name	サーバ グループ名。これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルト リストにあるアカウンティング方式を、アカウンティング サービス用に指定します。

start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。start アカウンティング レコードはバックグラウンドで送信されます。アカウンティング サーバが start accounting 通知を受け取ったかどうかには関係なく、要求されたユーザ プロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティング レコードをイネーブルにして、アカウンティング レコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップ サーバのリストを使用して最初のサーバを識別します。
group	アカウンティング サービスに使用するサーバ グループを指定します。有効なサーバ グループ名は次のとおりです。 • 名前：サーバ グループの名前。 • **radius**：すべての RADIUS ホストの一覧。 • **tacacs+**：すべての TACACS+ ホストの一覧。 **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの **group** キーワードより多くの値を入力できます。
radius	（任意）RADIUS アカウンティングをイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

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

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

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。

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

aaa accounting identity

IEEE 802.1x、MAC 認証バイパス（MAB）、およびWeb認証セッションの認証、認可、およびアカウンティング（AAA）アカウンティ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、**aaa accounting identity** コマンドを使用します。IEEE 802.1x アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

group	アカウンティング サービスに使用するサーバ グループを指定します。有効なサーバ グループ名は次のとおりです。 • 名前：サーバ グループの名前。 • **radius**：すべての RADIUS ホストの一覧。 • **tacacs+**：すべての TACACS+ ホストの一覧。 **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの **group** キーワードより多くの値を入力できます。
radius	（任意）RADIUS 認証をイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

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

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

AAA アカウンティング アイデンティティをイネーブルにするには、ポリシー モードをイネーブルにする必要があります。ポリシー モードをイネーブルにするには、特権 EXEC モードで **authentication display new-style** コマンドを入力します。

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

```
Device# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
```

```
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

Device# configure terminal
Device(config)# aaa accounting identity default start-stop group radius
```

aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで使用する認証、認可、およびアカウンティング（AAA）方式を指定するには、スイッチ スタックまたはスタンドアロン スイッチ上のグローバル 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**} *method1*

no aaa authentication dot1x {**default**} *method1*

構文の説明

default	ユーザがログインするときのデフォルトの方法。この引数に続いてリストされた認証方式が使用されます。
method1	サーバ認証を指定します。認証用にすべての RADIUS サーバの一覧を使用するには、**group radius** キーワードを入力します。 （注） コマンドラインのヘルプ文字列には他のキーワードが表示されますが、サポートされているのは **default** および **group radius** キーワードのみです。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために特定の順序で試みる方式を指定します。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 コマンドを入力して 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一覧を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

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。

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

aaa authorization

ネットワークへのユーザ アクセスを制限する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 **aaa authorization** コマンドを使用します。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。

aaa authorization {**auth-proxy** | **cache** | **commands***level* | **config-commands** | **configuration** |**console** | **credential-download** |**exec** | **multicast** | **network** | **onep** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** |**subscriber-service** | **template**} {**default** | *list_name*} [*method1* [*method2...*]]

aaa authorization { **auth-proxy** | **cache** | **commands***level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **reverse-access** |**template**} {**default** | *list_name*} [*method1* [*method2...*]]

no aaa authorization { **auth-proxy** | **cache** | **commands***level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **reverse-access** |**template**} {**default** | *list_name*} [*method1* [*method2...*]]

構文の説明

auth-proxy	認証プロキシ サービスに許可を実行します。
cache	認証、許可、アカウンティング（AAA）サーバを設定します。
commands	指定した特権レベルですべてのコマンドの許可を実行します。
level	許可が必要な特定のコマンド レベル。有効な値は 0 ～ 15 です。
config-commands	コンフィギュレーションモードで入力されたコマンドを許可するかどうかを決定する許可を実行します。

設定	AAA サーバから設定をダウンロードします。
console	AAA サーバのコンソール許可をイネーブルにします。
credential-download	Local/RADIUS/LDAP から EAP クレデンシャルをダウンロードします。
exec	AAA サーバのコンソール許可をイネーブルにします。
multicast	AAA サーバからマルチキャスト設定をダウンロードします。
network	シリアル ライン インターネット プロトコル（SLIP）、PPP（ポイントツーポイント プロトコル）、PPP ネットワーク コントロール プログラム（NCP）、AppleTalk Remote Access（ARA）など、すべてのネットワーク関連サービス要求について許可を実行します。
onep	ONEP サービスに許可を実行します。
reverse-access	リバース Telnet などの逆アクセス接続の許可を実行します。
template	AAA サーバのテンプレート許可をイネーブルにします。
default	このキーワードに続く許可方式のリストを許可のデフォルト方式リストとして使用します。
list_name	許可方式リストの名前の指定に使用する文字列です。
method1[*method2...*]	（任意）許可に使用する 1 つまたは複数の許可方式を指定します。方式には、次の表に示すキーワードのどれでも指定できます。

コマンド デフォルト

すべてのアクションに対する許可がディセーブルになります（方式キーワード **none** と同等）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

aaa authorization コマンドを使用して、許可をイネーブルにし、名前付きの方式リストを作成します。このリストにはユーザが特定の機能にアクセスするときに使用できる許可方式が定義されます。許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、一定順序で使用する必要がある許可方式（RADIUS、TACACS+ など）を示す名前付きリストです。方式リストを使用すると、許可に使用するセキュリティ プロトコルを 1 つ以上指定できるため、最初の方式が失敗した場合のバックアップ システムを確保できます。Cisco IOS ソフトウェアでは、特定のネットワーク サービスについてユーザを許可するために最初の方式が使用されます。その方式が応答しない場合、方式リストの次の方式が選択されます。このプロセスは、リスト内の許可方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。

（注） Cisco IOS ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次の許可方式が試行されます。このサイクルの任意の時点で許可が失敗した場合（つまり、セキュリティ サーバまたはローカル ユーザ名データベースからユーザ サービスの拒否応答が返される場合）、許可プロセスは停止し、その他の許可方式は試行されません。

特定の許可の種類の **aaa authorization** コマンドを、名前付き方式リストを指定しないで発行した場合、名前付き方式リストが明示的に定義されているものを除いて、すべてのインターフェイスまたは回線（この許可の種類が適用される）にデフォルトの方式リストが自動的に適用されます（定義済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、許可は実行されません。RADIUS サーバからの IP プールのダウンロードを許可するなどの発信許可は、デフォルトの許可方式リストを使用して実行する必要があります。

aaa authorization コマンドを使用して、*list-name* 引数および *method* 引数に値を入力してリストを作成します。*list-name* にはこのリストの名前として使用する任意の文字列（すべての方式名を除く）を指定し、*method* には特定の順序で試行される許可方式のリストを指定します。

（注） 次の表に、以前定義済みの RADIUS サーバまたは TACACS+ サーバのセットを参照する **group***group-name* 方式、**group ldap** 方式、**group radius** 方式、および **group tacacs+** 方式を示します。ホスト サーバを設定するには、**radius-server host** コマンドおよび **tacacs-server host** コマンドを使用します。サーバの名前付きグループを作成するには、**aaa group server radius** コマンド、**aaa group server ldap** コマンドおよび **aaa group server tacacs+** コマンドを使用します。

この表では、method キーワードについて説明します。

表 *38* : *AAA* 許可方式

キーワード	説明
cache*group-name*	キャッシュ サーバ グループを許可に使用します。
group*group-name*	アカウンティングに、**server group***group-name* コマンドで定義される RADIUS または TACACS+ サーバのサブセットを使用します。
group ldap	許可にすべての Lightweight Directory Access Protocol（LDAP）サーバのリストを使用します。
group radius	**aaa group server radius** コマンドで定義されるすべての RADIUS サーバのリストを認証に使用します。
grouptacacs+	**aaa group server tacacs+** コマンドで定義されるすべての TACACS+ サーバのリストを認証に使用します。
if-authenticated	許可された場合、ユーザは要求した機能にアクセスできます。 （注） **if-authenticated** 方式は終端の方式です。したがって、方式としてリストされている場合、その後にリストされたどの方式も評価されません。
local	許可にローカル データベースを使用します。
none	許可が行われないことを示します。

Cisco IOS ソフトウェアは、許可について次の方式をサポートします。

- Cache Server Groups：ルータはキャッシュ サーバ グループを調べて、特定の権限をユーザに許可します。
- If-Authenticated：ユーザが認証に成功した場合、ユーザは要求した機能にアクセスできます。
- Local：ルータまたはアクセス サーバは、**username** コマンドの定義に従ってローカル データベースに問い合わせ、特定の権限をユーザに許可します。ローカルデータベースでは制御できるのは、一部の機能だけです。
- None：ネットワーク アクセス サーバは、許可情報を要求しません。許可は、この回線/インターフェイスで実行されません。

- RADIUS：ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの許可情報を要求します。RADIUS認可では、属性を関連付けることでユーザに固有の権限を定義します。属性は適切なユーザとともに RADIUS サーバ上のデータベースに保存されます。
- TACACS+：ネットワーク アクセス サーバは、TACACS+ セキュリティ デーモンと許可情報を交換します。TACACS+ 許可は、属性値（AV）ペアを関連付けることでユーザに特定の権限を定義します。属性ペアは適切なユーザとともに TACACS+ セキュリティ サーバのデータベースに保存されます。

方式リストは、要求されている許可のタイプによって異なります。AAA は 5 種類の許可方式をサポートしています。

- Commands：ユーザが発行する EXEC モード コマンドに適用します。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- EXEC：ユーザ EXEC ターミナル セッションに関連付けられた属性に適用します。
- Network：ネットワーク接続に適用します。ネットワーク接続には、PPP、SLIP、または ARA 接続が含まれます。

（注） **aaa authorization config-commands** コマンドを設定して、先頭に **do** コマンドが追加される EXEC コマンドを含む、グローバル コンフィギュレーション コマンドを許可する必要があります。

- Reverse Access：リバース Telnet セッションに適用されます。
- Configuration：AAA サーバからダウンロードされた設定に適用されます。

名前付き方式リストを作成すると、指定した許可タイプに対して特定の許可方式リストが定義されます。

定義されると、方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。

authorization コマンドにより、許可プロセスの一環として、一連の AV のペアを含む要求パケットが RADIUS または TACACS+ デーモンに送信されます。デーモンは、次のいずれかのアクションを実行できます。

- 要求をそのまま受け入れます。
- 要求を変更します。
- 要求および許可を拒否します。

サポートされる RADIUS 属性のリストについては、RADIUS 属性のモジュールを参照してください。サポートされる TACACS+ の AV ペアのリストについては、TACACS+ 属性値ペアのモジュールを参照してください。

（注） 次の5個のコマンドは、特権レベル0と対応しています。**disable**、**enable**、**exit**、**help**、**logout**。特権レベルのAAA認証を0より大きい値に設定した場合、これらの5個のコマンドは特権レベル コマンド セットに含まれません。

次に、PPPを使用するシリアル回線にRADIUSの許可を使用するように指定するmygroupというネットワーク許可方式リストを定義する例を示します。RADIUSサーバが応答しない場合、ローカル ネットワークの許可が実行されます。

```
Device(config)#  aaa authorization network mygroup group radius local
```

aaa new-model

認証、認可、およびアカウンティング（AAA）アクセス制御モデルを有効にするには、グローバル コンフィギュレーション モードで**aaanew-model**コマンドを使用します。AAAアクセス制御モデルを無効にするには、このコマンドの**no**形式を使用します。

aaa new-model

no aaa new-model

構文の説明

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

AAAが有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドがCisco Catalyst 3850シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドにより、AAAアクセス制御システムが有効になります。

仮想端末回線（VTY）に関して **login local** コマンドが設定されている場合、**aaa new-model** コマンドを削除するときは、スイッチをリロードしてデフォルト設定または **login** コマンドを取得する必要があります。スイッチをリロードしない場合、スイッチは、VTY ではデフォルトで **login local** コマンドに設定されます。

（注） **aaa new-model** コマンドを削除することは推奨されません。

次に、この制限の例を示します。

```
Switch(config)# aaa new-model
Switch(config)# line vty 0 15
Switch(config-line)# login local
Switch(config-line)# exit
Switch(config)# no aaa new-model
Switch(config)# exit
Switch# show running-config | b line vty

line vty 0 4
 login local  !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

次に、AAA を初期化する例を示します。

```
Switch(config)# aaa new-model
Switch(config)#
```

関連コマンド

コマンド	説明
aaaaccounting	課金またはセキュリティ目的のために、要求されたサービスのAAAアカウンティングをイネーブルにします。
aaaauthenticationarap	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
aaaauthenticationenabledefault	ユーザが特権コマンドレベルにアクセスできるかどうかを決定するAAA認証を有効にします。
aaaauthenticationlogin	ログイン時の AAA 認証を設定します。
aaaauthenticationppp	PPPを実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
aaaauthorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。

access-session mac-move deny

デバイス 上での MAC 移動をディセーブルにするには、**access-session mac-move deny** グローバル 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。

access-session mac-move deny

no access-session mac-move deny

構文の説明

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
Cisco IOS XE 3.2SE	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 **no** 形式を使用すると、認証済みホストをデバイス上の認証対応ポート（MAC 認証バイパス [MAB]、802.1x、または Web-auth）間で移動することができます。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。

次の例では、デバイス上で MAC 移動をイネーブルにする方法を示します。

```
Device(config)# no access-session mac-move deny
```

関連コマンド

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

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

drop	指定された条件に一致する場合に、パケットをドロップします。

forward	指定された条件に一致する場合に、パケットを転送します。

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
Cisco IOS XE 3.2SE	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、一致条件でのアクセス コントロール リスト（ACL）名の設定など、アクセス マップを定義した後に、そのマップを VLAN に適用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 access-map** 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します。**action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

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

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。

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。

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

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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication host-mode {**multi-auth** | **multi-domain** | **multi-host** |**single-host**}

no authentication host-mode

構文の説明

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

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
Cisco IOS XE 3.2SE	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 フォン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。

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。

```
Device(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。

```
Device(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。

```
Device(config-if)# authentication host-mode multi-host
```

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

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

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

authentication mac-move permit

デバイス上での 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。MAC 移動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 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 移動は無効になっています。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

これはレガシー コマンドです。新しいコマンドは **access-session mac-move deny** です。

このコマンドを使用すると、デバイス上の認証対応ポート（MAC認証バイパス[MAB]、802.1x、またはWeb-auth）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。

次の例では、デバイス上でMAC 移動をイネーブルにする方法を示します。

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

関連コマンド

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

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

認証優先

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。デフォルトに戻るには、**no** 形式のコマンドを使用します。

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

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

構文の説明

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

コマンド デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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（MAB）、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。

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

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

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

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

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event fail	認証マネージャが認証エラーを認識されないユーザ クレデンシャルの結果として処理する方法を指定します。

コマンド	説明
authentication event no-response action	認証マネージャが認証エラーを応答のないホストの結果として処理する方法を指定します。
authentication event server alive action reinitialize	以前に到達不能であった認証、許可、アカウンティングサーバが使用可能になったときに認証マネージャセッションを再初期化します。
authentication event server dead action authorize	認証、許可、アカウンティングサーバが到達不能になったときに認証マネージャ セッションを許可します。
authentication fallback	Web 認証のフォール バック方式をイネーブルにします。
authentication host-mode	ホストの制御ポートへのアクセスを許可します。
authentication open	ポートでオープン アクセスをイネーブルにします。
authentication order	認証マネージャがポート上のクライアントの認証を試みる順序を指定します。
authentication periodic	ポートの自動再認証をイネーブルにします。
authentication port-control	制御ポートの許可ステートを設定します。
authentication timer inactivity	機能しない認証マネージャセッションを強制終了するまでの時間を設定します。
authentication timer reauthenticate	認証マネージャが許可ポートの再認証を試みる間隔を指定します。
authentication timer restart	認証マネージャが無許可ポートの認証を試みる間隔を指定します。
authentication violation	ポート上でセキュリティ違反が生じた場合に取るアクションを指定します。
mab	ポートの MAC 認証バイパスをイネーブルにします。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	現在の認証マネージャ セッションに関する情報を表示します。
show authentication sessions interface	特定のインターフェイスの認証マネージャ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されたとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続された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 **authentication violation** コマンドを使用します。

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

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

構文の説明

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

コマンド デフォルト

Authentication violation shutdown 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

ポート上でセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

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。

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

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

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

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

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

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

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

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

cisp enable

スイッチ上で Client Information Signalling Protocol（CISP）を有効にして、サプリカント スイッチのオーセンティケータとして機能し、オーセンティケータ スイッチのサプリカントとして機能するようにするには、**cisp enable** グローバル コンフィギュレーション コマンドを使用します。

cisp enable

no cisp 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

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

使用上のガイドライン

オーセンティケータとサプリカント スイッチの間のリンクはトランクです。両方のスイッチで 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に MD5 チェックサムの不一致エラーにならないようにするために、次の点を確認してください。

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

次の例では、CISP をイネーブルにする方法を示します。

```
Device(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentials*profile*	プロファイルをサプリカント スイッチに設定します。
dot1x supplicant force-multicast	802.1X サプリカントがマルチキャスト パケットを送信するように強制します。
dot1x supplicant controlled transient	802.1X サプリカントによる制御アクセスを設定します。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

clear errdisable interface vlan

error-disabled 状態になっていた 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

interface-id	インターフェイスを指定します。
vlan list	（任意）再びイネーブルにする VLAN のリストを指定します。VLAN リストを指定しない場合は、すべての VLAN が再びイネーブルになります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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** インターフェイス コマンドを使用して VLAN の error-disabled をクリアできます。

次の例では、ギガビット イーサネット ポート 4/0/2 で errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

関連コマンド

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

clear mac address-table

特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、スタック メンバ上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを MAC アドレス テーブルから削除するには、**clear mac address-table** コマンドを特権 EXEC モードで使用します。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*] | **move update** | **notification**}

構文の説明

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

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 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。

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。

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

関連コマンド

コマンド	説明
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
mac address-table move update {**receive** | **transmit**}	スイッチ上の MAC アドレス テーブル移行更新を設定します。
show mac address-table	MAC アドレス テーブルのスタティック エントリおよびダイナミック エントリを表示します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。
show mac address-table notification	**interface** キーワードが追加されると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。

コマンド	説明
snmp trap mac-notification change	特定のインターフェイスの SNMP MAC アドレス通知トラップをイネーブルにします。

cts manual

Cisco TrustSec セキュリティ（CTS）のインターフェイスを手動で有効にするには、インターフェイス コンフィギュレーション モードで **cts manual** コマンドを使用します。

cts 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

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが変更され、いくつかのオプションが追加されました。
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

リンクにポリシーおよびセキュリティ アソシエーション プロトコル（SAP）を設定する TrustSec 手動インターフェイス コンフィギュレーションを開始するには、**cts manual** コマンドを使用します。

cts manual コマンドが設定された場合、802.1X 認証はリンクで実行されません。ポリシーを定義し、リンクに適用するには、 **policy** サブコマンドを使用します。デフォルトでは、ポリシーは適用されません。MACsec リンク間暗号化を設定するには、SAP ネゴシエーション パラメータを定

義する必要があります。デフォルトでは、SAPは有効になっていません。同じSAPペアワイズマスター キー（PMK）をリンクの両端で設定する必要があります（つまり、共有秘密）。

次に、Cisco TrustSec 手動モードを開始する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# cts manual
Switch(config-if-cts-manual))#
```

次に、インターフェイスから CTS 手動設定を削除する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# no cts manual
```

関連コマンド

コマンド	説明
propagate sgt（cts manual）	Cisco TrustSec セキュリティ（CTS）インターフェイスで、レイヤ2でのセキュリティ グループ タグ（SGT）伝播を有効にします。
sap mode-list（cts manual）	PMK インターフェイスと SAP インターフェイスの間での MACsec リンク暗号化のネゴシエーションのために、それらの認証と暗号化モードを手動で指定します。
show cts interface	Cisco TrustSecインターフェイス設定統計情報を表示します。

cts role-based enforcement

Cisco TrustSec ロールベース（セキュリティ グループ）アクセス コントロール適用を有効にするには、グローバル コンフィギュレーション モードで **ctsrole-basedenforcement** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

cts role-based enforcement[**logging-interval***interval*| **vlan-list**{**all**| *vlan-ID*[**,**] [**-**]}]

no cts role-based enforcement[**logging-interval***interval*| **vlan-list**{**all**| *vlan-ID*[**,**] [**-**]}]

構文の説明

logging-interval*interval*	（任意）セキュリティ グループ アクセス コントロール リスト（SGACL）のロギング間隔を設定します。*interval* 引数の有効な値は 5 ～ 86400 秒です。デフォルトは 300 秒です。
vlan-list	（任意）ロールベース ACLが適用される VLAN を設定します。

all	（任意）すべての VLAN を指定します。
vlan-ID	（任意）VLAN ID。有効な値は 1 ～ 4094 です。
,	（任意）別の VLAN をカンマで区切って指定します。
-	（任意）VLAN の範囲をハイフンで区切って指定します。

コマンド デフォルト

ロールベース アクセス コントロールは適用されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

（注） RBACL と SGACL は互換的に使用されます。

システムで Cisco TrustSec 対応インターフェイスの SGACL 適用をグローバルに有効または無効にするには、**ctsrole-basedenforcement** コマンドを使用します。

特定のフローのログが出力されるデフォルトの間隔は 300 秒です。デフォルトの間隔を変更するには、**logging-interval** キーワードを使用します。ロギングは、Cisco ACE アプリケーション コントロール エンジンに **logging** キーワードがある場合にのみトリガーされます。

VLAN での SGACL 適用は、デフォルトでは有効になっていません。スイッチ仮想インターフェイス（SVI）でレイヤ 2 スイッチド パケットおよびレイヤ 3 スイッチド パケットの SGACL 適用を有効または無効にするには、**ctsrole-basedenforcementvlan-list** コマンドを使用します。

vlan-ID 引数には単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲を指定できます。

SGACL が適用される VLAN で SVI がアクティブである場合、SGACL はその VLAN 内のレイヤ 2 とレイヤ 3 の両方のスイッチド パケットに適用されます。レイヤ 3 スイッチングは SVI を使用しない VLAN 内では使用できないため、SVI を使用しない場合、SGACL はレイヤ 2 スイッチド パケットにのみ適用されます。

次に、SGACL ロギング間隔を設定する例を示します。

```
Switch(config)# cts role-based enforcement logging-interval 90
Switch(config)# logging rate-limit

May 27 10:19:21.509: %RBM-6-SGACLHIT:
ingress_interface='GigabitEthernet1/0/2' sgacl_name='sgacl2' action='Deny'
protocol='icmp' src-ip='16.16.1.3' src-port='8' dest-ip='17.17.1.2' dest-port='0'
sgt='101' dgt='202' logging_interval_hits='5'
```

関連コマンド

コマンド	説明
loggingrate-limit	1 秒間にログに記録されるメッセージの割合を制限します。
showctsrole-basedpermissions	SGACL 権限リストを表示します。

cts role-based l2-vrf

レイヤ 2 VLAN の Virtual Routing and Forwarding（VRF）インスタンスを選択するには、グローバル コンフィギュレーション モードで **ctsrole-basedl2-vrf** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

cts role-based l2-vrf *vrf-name***vlan-list** {**all**| *vlan-ID*} [**,**] [**-**]

no cts role-based l2-vrf *vrf-name***vlan-list** {**all**| *vlan-ID*} [**,**] [**-**]

構文の説明

vrf-name	VRF インスタンスの名前。
vlan-list	VRF インスタンスに割り当てられる VLAN のリストを指定します。
all	すべての VLAN を指定します。
vlan-ID	VLAN ID。有効な値は 1 ～ 4094 です。
,	（任意）別の VLAN をカンマで区切って指定します。
-	（任意）VLAN の範囲をハイフンで区切って指定します。

コマンド モード

グローバル コンフィギュレーション（config）

VRF インスタンスは選択されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 引数には単一の VLAN ID、カンマで区切られた VLAN ID のリスト、またはハイフンで区切られた VLAN ID の範囲を指定できます。

all キーワードは、ネットワーク デバイスによってサポートされている VLAN の全範囲と同等です。**all** キーワードは、不揮発性生成（NVGEN）プロセスで保持されません。

ctsrole-basedl2-vrf コマンドが同じ VRF に複数回実行される場合、入力される連続した各コマンドは、指定された VRF に VLAN ID を追加します。

ctsrole-basedl2-vrf コマンドで設定された VRF 割り当ては、VLAN がレイヤ 2 VLAN として維持されている間はアクティブです。VRF の割り当てがアクティブな間に、学習した IP-SGT バインディングも VRF と IP プロトコル バージョンに関連付けられた転送情報ベース（FIB）テーブルに追加されます。VLAN のスイッチ仮想インターフェイス（SVI）がアクティブになると、VRF から VLAN への割り当てが非アクティブになり、VLAN で学習されたすべてのバインディングが SVI の VRF に関連付けられた FIB テーブルに移動されます。

SVI インターフェイスを設定するには **interface vlan** コマンドを使用し、VRF インスタンスをインターフェイスに関連付けるには **vrfforwarding** コマンドを使用します。

VRF から VLAN への割り当ては、割り当てが非アクティブになっても保持されます。SVI が削除された、または SVI の IP アドレスの変更された場合に再アクティブ化されます。再アクティブ化された場合、IP-SGT バインディングは、SVI の FIB に関連付けられた FIB テーブルから、**ctsrole-basedl2-vrf** コマンドによって割り当てられた VRF に関連付けられた FIB テーブルに戻されます。

次に、VRF インスタンスに割り当てられる VLAN のリストを選択する例を示します。

```
Switch(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

次に、SVI インターフェイスを設定し、VRF インスタンスを関連付ける例を示します。

```
Switch(config)# interface vlan 101
Switch(config-if)# vrf forwarding vrf1
```

関連コマンド

コマンド	説明
interfacevlan	VLAN インターフェイスを設定します。

コマンド	説明
vrfforwarding	VRFインスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。
showctsrole-basedpermissions	SGACL 権限リストを表示します。

cts role-based monitor

ロールベース（セキュリティ グループ）アクセス リスト モニタリングを有効にするには、グローバル コンフィギュレーション モードで **ctsrole-basedmonitor** コマンドを使用します。ロールベース アクセス リスト モニタリ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。

cts role-based monitor {**all**| **permissions**| {**default**| **from**{*sgt*| **unknown**}} **to**{*sgt*| **unknown**} [**ipv4**]}
no cts role-based monitor {**all**| **permissions**| {**default**| **from**{*sgt*| **unknown**}} **to**{*sgt*| **unknown**} [**ipv4**]}

構文の説明

all	すべての宛先タグへのすべての送信元タグの権限をモニタします。
permissions	1 つの送信元タグから 1 つの宛先タグへの権限をモニタします。
default	デフォルトの権限リストをモニタします。
from	フィルタリングされるトラフィックの送信元グループ タグを指定します。
sgt	セキュリティ グループ タグ（SGT）有効値は 2 ～ 65519 です。
unknown	未知の送信元または宛先グループ タグ（DST）を指定します。
ipv4	（任意）IPv4 プロトコルを指定します。

コマンド デフォルト

ロールベース アクセス コントロール モニタリングは有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

グローバル モニタ モードを有効にするには、**ctsrole-basedmonitorall** コマンドを使用します。**ctsrole-basedmonitorall** コマンドが設定されている場合、**showctsrole-basedpermissions** コマンドの出力には、設定されているすべてのポリシーのモニタ モードが true と表示されます。

次に、送信元タグから宛先タグへの SGACL モニタを設定する例を示します。

```
Switch(config)# cts role-based monitor permissions from 10 to 11
```

関連コマンド

コマンド	説明
showctsrole-basedpermissions	SGACL 権限リストを表示します。

cts role-based permissions

1 つの送信元グループから 1 つの宛先グループへの権限を有効にするには、グローバル コンフィギュレーション モードで **ctsrole-basedpermissions** コマンドを使用します。権限を削除するには、このコマンドの **no** 形式を使用します。

cts role-based permissions {**defaultipv4**| **from** {*sgt*| **unknown**} **to** {*sgt*| **unknown**} {**ipv4**} {*rbacl-name* [*rbacl-name....*]}}

no cts role-based permissions {**default**[**ipv4**] | **from** {*sgt*| **unknown**} **to** {*sgt*| **unknown**} [**ipv4**]}

構文の説明

default	デフォルトの権限リストを指定します。セキュリティ グループ アクセス コントロール リスト（SGACL）権限が静的または動的に設定されていないすべてのセル（SGT ペア）は、デフォルトのカテゴリに属します。
ipv4	IPv4 プロトコルを指定します。
from	フィルタリングされるトラフィックの送信元グループ タグを指定します。
sgt	セキュリティ グループ タグ（SGT）有効値は 2 ～ 65519 です。

unknown	未知の送信元または宛先グループ タグを指定します。
rbacl-name	ロールベース アクセス コントロール リスト(RBACL)またはSGACLの名前。この設定では最大 16 の SGACL を指定できます。

コマンド デフォルト

1 つの送信元グループから 1 つの宛先グループへの権限は有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

特定の送信元グループ タグ（SGT）、宛先グループ タグ（DGT）ペアの SGACL のリストを定義したり、置き換えたり、削除したりするには、**ctsrole-basedpermissions** コマンドを使用します。このポリシーは、同じDGTまたはSGTに対するダイナミックなポリシーがないかぎり有効です。

ctsrole-basedpermissionsdefault コマンドでは、同じDGTに対するダイナミックなポリシーがないかぎり、デフォルト ポリシーの SGACL のリストを定義したり、置き換えたり、削除したりすることができます。

次に、宛先グループの権限を有効にする例を示します。

```
Switch(config)# cts role-based permissions from 6 to 6 mon_2
```

関連コマンド

コマンド	説明
showctsrole-basedpermissions	SGACL 権限リストを表示します。

deny（MAC アクセス リスト コンフィギュレーション）

条件が一致した場合に非IPトラフィックが転送されるのを防止するには、スイッチ スタックまたはスタンドアロン スイッチ上で **deny** MAC アクセスリスト コンフィギュレーション コマンドを使用します。名前付き MAC アクセス リストから拒否条件を削除するには、このコマンドの **no** 形式を使用します。

deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **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**][**cos** *cos*]

no deny {**any** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **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**][**cos** *cos*]

構文の説明

any	すべての送信元または宛先 MAC アドレスを拒否します。
host*src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非IPトラフィックは拒否されます。
host*dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非IPトラフィックは拒否されます。
type mask	（任意）パケットの EtherType 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。 type には、0 ～ 65535 の 16 進数を指定できます。 mask は、一致をテストする前に EtherType に適用される don’t care ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。
amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定します。

dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを指定します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	（任意）EtherType DEC-Diagnostic を指定します。
dsm	（任意）EtherType DEC-DSM を指定します。
etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。
lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します。
lsap*lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を指定します。
mop-dump	（任意）EtherType DEC-MOP Dump を指定します。
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NetBIOS）を指定します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を指定します。
vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）10 進数、16 進数、または 8 進数の任意の Ethertype である EtherType Xerox Network Systems（XNS）プロトコル スイート（0 ～ 65535）を指定します。

cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までのサービス クラス（CoS）値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。

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
Cisco IOS XE 3.2SE	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 アクセス リスト コンフィギュレーション モードを開始するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

host キーワードを使用した場合、アドレス マスクは入力できません。**host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

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。

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。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表に一覧表示します。

表 *39* : *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

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novel 名	
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

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。

```
Device(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。

```
Device(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。

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

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

関連コマンド

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
permit	MAC アクセスリスト コンフィギュレーションから許可します。 条件が一致した場合に非 IP トラフィックが転送されるのを許可します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

device-role（IPv6 スヌーピング）

ポートに接続されているデバイスのロールを指定するには、IPv6 スヌーピング コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {**node** | **switch**}

構文の説明

node	接続されたデバイスのロールをノードに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはノードです。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。デフォルトでは、デバイスのロールはノードです。

switch キーワードは、リモート デバイスがスイッチであり、ローカル スイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインディング エントリは、trunk_port プリファレンス レベルでマークされます。ポートが trusted ポートに設定されている場合、バインディング エントリは trunk_trusted_port プリファレンス レベルでマークされます。

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、デバイスをノードとして設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
```

device-role（IPv6 ND 検査）

ポートに接続されているデバイスのロールを指定するには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードで **device-role** コマンドを使用します。

構文の説明

host	接続されたデバイスのロールをホストに設定します。

device-role {**host** | **monitor** | **router** | **switch**}

monitor	接続されたデバイスのロールをモニタに設定します。
router	接続されたデバイスのロールをルータに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはホストです。

コマンド モード

ND インスペクション 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。デフォルトでは、デバイスのロールはホストであるため、すべての着信ルータ アドバタイズメントとリダイレクト メッセージはブロックされます。デバイス ロールが **router** キーワードを使用してイネーブルになっている場合、このポートですべてのメッセージ（ルータ送信要求（RS）、ルータ アドバタイズメント（RA）、またはリダイレクト）が許可されます。

router または **monitor** キーワードが使用されている場合、マルチキャストの RS メッセージは限定ブロードキャストがイネーブルかどうかに関係なく、ポート上でブリッジされます。ただし、monitor キーワードは着信 RA またはリダイレクト メッセージを許可しません。monitor キーワードを使用すると、これらのメッセージを必要とするデバイスがそれらを受け取ります。

switch キーワードは、リモート デバイスがスイッチであり、ローカル スイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインド エントリは、trunk_port プリファレンス レベルでマークされます。ポートが trusted ポートに設定されている場合、バインディング エントリは trunk_trusted_port プリファレンス レベルでマークされます。
次に、Neighbor Discovery Protocol（NDP）ポリシー名を policy1 と定義し、デバイスを ND インスペクション ポリシー コンフィギュレーション モードにして、デバイスをホストとして設定する例を示します。

```
Device(config)#  ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
```

device-tracking policy

スイッチ統合型セキュリティ機能（SISF）ベースの IP デバイス トラッキング ポリシーを設定するには、グローバル コンフィギュレーション モードで **device-tracking** コマンドを使用します。デバイス トラッキング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

device -tracking policy *policy-name*

no device-tracking policy *policy-name*

構文の説明

policy-name	デバイス トラッキング ポリシーのユーザ定義名。ポリシー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

デバイス トラッキング ポリシー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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

デバイス トラッキング ポリシーを作成するには、SISF ベースの **device-tracking policy** コマンドを使用します。**device-tracking policy** コマンドがイネーブルの場合、コンフィギュレーション モードが デバイストラッキング コンフィギュレーション モードに変更されます。このモードでは、管理者が次のファーストホップ セキュリティ コマンドを設定できます。

- （任意）**device-role**{**node**]|**switch**}：ポートに接続されたデバイスのロールを指定します。デフォルトは **node** です。
- （任意）**limit address-count***value*：ターゲットごとに許可されるアドレス数を制限します。
- （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。
- （任意）**destination-glean**{**recovery**|**log-only**}[**dhcp**]}：データ トラフィックの送信元アドレス グリーニングによるバインディング テーブルの回復をイネーブルにします。

- （任意）**data-glean**{**recovery**| **log-only**}[**dhcp** | **ndp**]}：送信元アドレスまたはデータ アドレスのグリーニングを使用したバインディング テーブルの回復をイネーブルにします。
- （任意）**security-level**{**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。

  glean：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。

  guard：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これがデフォルトのオプションです。

  inspect：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。

- （任意）**tracking** {**disable** | **enable**}：トラッキング オプションを指定します。
- （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。

次に、デバイストラッキング ポリシーを設定する例を示します。

```
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
```

dot1x critical（グローバル コンフィギュレーション）

IEEE 802.1X クリティカル認証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。

dot1x critical eapol

構文の説明

eapol	スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。

コマンド デフォルト

eapol 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するよう指定する例を示します。

```
Device(config)# dot1x critical eapol
```

dot1x max-start

もう一方の端で802.1Xが認識されないと判断されるまでにサプリカントがクライアントに送信する（応答が受信されないと想定）Extensible Authentication Protocol over LAN（EAPOL）開始フレーム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-start** コマンドを使用します。最大回数の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。

dot1x max-start *number*

no dot1x max-start

構文の説明

number	ルータが EAPOL 開始フレームを送信する最大回数を指定します。1 ～ 10 の値を指定できます。デフォルトは 3 です。

コマンド デフォルト

デフォルトの最大数の設定は 3 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
Cisco IOS XE 3.2SE	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 **switchport mode access** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

次に、EAPOL 開始要求の最大数が 5 に設定されている例を示します。

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x max-start 5
```

dot1x pae

Port Access Entity（PAE）タイプを設定するには、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。設定された PAE タイ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。

dot1x pae {**supplicant** | **authenticator**}

no dot1x pae {**supplicant** | **authenticator**}

構文の説明

supplicant	インターフェイスはサプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。
authenticator	インターフェイスはオーセンティケータとしてだけ動作し、サプリカント向けのメッセージに応答しません。

コマンド デフォルト

PAE タイプ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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

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。

次に、インターフェイスがサプリカントとして動作するように設定されている例を示します。

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x pae supplicant
```

dot1x supplicant controlled transient

認証中に802.1xサプリカントポートへのアクセスを制御するには、グローバル コンフィギュレーション モードで **dot1x supplicant controlled transient** コマンドを使用します。認証中にサプリカントのポートを開くには、このコマンドの **no** 形式を使用します。

dot1x supplicant controlled transient

no dot1x supplicant controlled transient

構文の説明

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

認証中に 802.1x サプリカントのポートへのアクセスが許可されます。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

使用上のガイドライン

デフォルトでは、BPCU ガードがイネーブルにされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する前にスパニングツリー プロトコル（STP）のブリッジ プロトコル データ ユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。Cisco IOS Release 15.0(1) SE 以降では、認証中にサプリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** 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、認証が完了する前にオーセンティケータ ポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートがブロックされます。認証に失敗すると、サプリカントのポートが開きます。**no dot1x supplicant controlled transient** 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、認証期間中にサプリカント ポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータ スイッチ ポートでイネーブルになっている場合、サプリカント スイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。

次に、認証の間にスイッチの 802.1x サプリカントのポートへのアクセスを制御する例を示します。

```
Device(config)# dot1x supplicant controlled transient
```

dot1x supplicant force-multicast

サプリカント スイッチでマルチキャストまたはユニキャストの Extensible Authentication Protocol over LAN（EAPOL）パケットを受信した場合に、常にマルチキャスト EAPOL パケットのみを送信するように強制するには、グローバル コンフィギュレーション モードで **dot1x supplicant force-multicast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x supplicant force-multicast

no dot1x supplicant force-multicast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

サプリカント スイッチは、ユニキャスト EAPOL パケットを受信すると、ユニキャスト EAPOL パケットを送信します。同様に、マルチキャスト EAPOL パケットを受信すると、EAPOL パケットを送信します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

使用上のガイドライン

Network Edge Access Topology（NEAT）がすべてのホスト モードで機能するようにするには、サプリカント スイッチ上でこのコマンドをイネーブルにします。

次の例では、サプリカント スイッチがオーセンティケータ スイッチにマルチキャスト EAPOL パケットを送信するように設定する方法を示します。

```
Device(config)# dot1x supplicant force-multicast
```

関連コマンド

コマンド	説明
cisp enable	スイッチの Client Information Signalling Protocol（CISP）をイネーブルにすることで、スイッチがサプリカント スイッチに対するオーセンティケータとして動作するようにします。
dot1x credentials	ポートに 802.1x サプリカント資格情報を設定します。
dot1x pae supplicant	インターフェイスがサプリカントとしてだけ機能するように設定します。

dot1x test eapol-capable

すべてのスイッチ ポート上の IEEE 802.1x のアクティビティをモニタリングして、IEEE 802.1x をサポートするポートに接続しているデバイスの情報を表示するには、スイッチ スタックまたはスタンドアロン スイッチの特権 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）クエリー対象のポートです。

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
Cisco IOS XE 3.2SE	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。

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。

```
Device# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

関連コマンド

コマンド	説明
dot1x test timeout*timeout*	IEEE 802.1x 準備クエリーに対する EAPOL 応答を待機するために使用されるタイムアウトを設定します。

dot1x test timeout

IEEE 802.1x 準備状態を照会しているポートからの EAPOL 応答の待機に使用されるタイムアウトを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、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

timeout	EAPOL 応答を待機する時間（秒）。指定できる範囲は 1 ～ 65535 秒です。

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
Cisco IOS XE 3.2SE	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。

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。

```
Device# dot1x test timeout 27
```

タイムアウト設定のステータスを確認するには、**show run** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x test eapol-capable [**interface***interface-id*]	すべての、または指定された IEEE 802.1x 対応ポートに接続するデバイスで IEEE 802.1x の準備が整っているかを確認します。

dot1x timeout

再試行タイムアウトの値を設定するには、グローバルコンフィギュレーションモードまたはインターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。再試行タイムアウ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。

dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds*| **ratelimit-period** *seconds*| **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout***seconds* | **tx-period** *seconds*}

構文の説明

auth-period*seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。

held-period*seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルト値は 60 です。
quiet-period*seconds*	認証情報の交換に失敗したあと、クライアントの再認証を試みるまでにオーセンティケータ（サーバ）が待機状態（HELD 状態）を続ける秒数を設定します。 有効な範囲は 1 ～ 65535 です。デフォルト値は 60 です。
ratelimit-period*seconds*	動作の不正なクライアント PC（たとえば、スイッチ処理電力の無駄につながる、EAP-START パケットを送信する PC）から送信される EAP-START パケットを抑制します。 • オーセンティケータはレート制限時間中、認証に成功したクライアントからの EAPOL-Start パケットを無視します。 • 有効な範囲は 1 ～ 65535 です。デフォルトでは、レート制限はディセーブルになっています。
server-timeout*seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 サーバが指定時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。
start-period*seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
supp-timeout*seconds*	EAP 要求 ID 以外のすべての EAP メッセージについて、オーセンティケータからホストへの再送信時間を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
tx-period*seconds*	クライアントに EAP 要求 ID パケットを再送信する間隔を（応答が受信されないものと仮定して）秒数で設定します。 • 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 • 802.1X パケットがサプリカントに送信され、そのサプリカントが再試行期間後に応答しなかった場合、そのパケットは再度送信されます。

コマンド デフォルト

定期的な再認証と定期的なレート制限が行われます。

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
Cisco IOS XE 3.2SE	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。

次に、さまざまな 802.1X 再送信およびタイムアウト時間が設定されている例を示します。

```
Device(config)# configure terminal
Device(config)# interface g1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
```

epm access-control open

アクセス コントロール リスト（ACL）が設定されていないポートにオープン ディレクティブを設定するには、グローバル コンフィギュレーション モードで **epm access-control open** コマンドを

使用します。オープン ディレクティブをディセーブルにするには、このコマンドの **no** 形式を使用します。

epm access-control open

no epm access-control open

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトのディレクティブが適用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 ACL が設定されたアクセス ポートに、認可ポリシーのないホストを許可するオープン ディレクティブを設定するには、このコマンドを使用します。このコマンドを設定しない場合、ポートは設定された ACL のポリシーをトラフィックに適用します。ポートにスタティック ACL が設定されていない場合、デフォルトおよびオープンの両方のディレクティブがポートへのアクセスを許可します。

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。

次の例では、オープン ディレクティブを設定する方法を示します。

```
Device(config)# epm access-control open
```

関連コマンド

コマンド	説明
show running-config	現在実行されているコンフィギュレーション ファイルの内容を表示します

ip access-list role-based

ロールベース（セキュリティ グループ）アクセス コントロール リスト（RBACL）を作成して、ロールベースACL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 access-list role-based** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

ip access-list role-based *access-list-name*

no ip access-list role-based *access-list-name*

構文の説明

access-list-name	セキュリティ グループ アクセス コントロール リスト（SGACL）の名前。

コマンド デフォルト

ロールベースの ACL は設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

SGACL ロギングの場合は、**permitiplog** コマンドを設定する必要があります。また、このコマンドは、ダイナミック SGACL のロギングを有効にするために、Cisco Identity Services Engine（ISE）でも設定する必要があります。

次に、IPv4トラフィックに適用できる SGACL を定義し、ロールベース アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
Switch(config)# ip access-list role-based rbacl1
Switch(config-rb-acl)# permit ip log
```

関連コマンド

コマンド	説明
permitiplog	設定されたエントリに一致するロギングを許可します。
showipaccess-list	現在のすべての IP アクセス リストの内容を表示します。

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、フォールバックプロファイルコンフィギュレーション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 *rule*

構文の説明

rule	IP アドミッション ルールの名前。

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

インターフェイス コンフィギュレーション

フォールバック プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

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。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(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。

```
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
```

ip admission name

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** 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 *name* {**consent** | **proxyhttp**} [**absolute timer** *minutes* | **inactivity-time***minutes* | **list**{*acl* | *acl-name*} | **service-policy type tag***service-policy-name*]

no ip admission name *name* {**consent** | **proxyhttp**} [**absolute timer** *minutes* | **inactivity-time***minutes* | **list**{*acl* | *acl-name*} | **service-policy type tag***service-policy-name*]

構文の説明

name	ネットワークアドミッション制御ルールの名前。
consent	認証プロキシ同意 Web ページを *admission-name* 引数で指定された IP アドミッション ルールに対応させます。
proxy http	Web 認証のカスタム ページを設定します。
absolute-timer *minutes*	（任意）外部サーバがタイム アウトするまでの経過時間（分）。
inactivity-time*minutes*	（任意）外部ファイル サーバが到達不能であると見なされるまでの経過時間（分）。
list	（任意）指定されたルールをアクセス コントロール リスト（ACL）に関連付けます。
acl	標準、拡張リストを指定のアドミッション制御ルールに適用します。値の範囲は 1～199、または拡張範囲で 1300 から 2699 です。

acl-name	名前付きのアクセスリストを指定のアドミッション制御ルールに適用します。
service-policy type tag	（任意）コントロール プレーン サービス ポリシーを設定できます。
service-policy-name	**policy-map type control tag***policyname* コマンド、キーワード、および引数を使用して設定されたコントロール プレーン タグのサービス ポリシー。このポリシー マップは、タグを受信したときのホストでの処理を適用するために使用されます。

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
Cisco IOS XE 3.2SE	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 コマンドにより、スイッチ上で Web 認証がグローバルにイネーブルになります。

スイッチ上で Web 認証を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上で Web 認証をイネーブルにします。

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。

```
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# ip admission rule
Device(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。

```
Device# configure terminal
Device(config)# ip admission name rule2 proxy http
Device(config)# fallback profile profile1
Device(config)# ip access group 101 in
Device(config)# ip admission name rule2
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x fallback profile1
Device(config-if)# end
```

関連コマンド

コマンド	説明
dot1x fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile	Web 認証のフォールバック プロファイルを作成します。
ip admission	ポートで Web 認証をイネーブルにします。
show authentication sessions interface *interface* **detail**	Web認証セッションのステータスに関する情報を表示します。
show ip admission	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。

ip device tracking maximum

レイヤ 2 アクセス ポートで IP デバイス トラッキング 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 **ip device tracking maximum** コマンドを使用します。最大値を削除するには、このコマンドの **no** 形式を使用します。

ip device tracking maximum *number*

no ip device tracking maximum

構文の説明

number	ポートのIPデバイストラッキングテーブルに作成するバインディングの数。範囲は 0（ディセーブル）～ 65535 です。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

最大値を削除するには、**no ip device tracking maximum** コマンドを使用します。

IP デバイス トラッキングをディセーブルにするには、**ip device tracking maximum 0** コマンドを使用します。

（注） このコマンドは、設定されている場合は常に IPDT を有効にします。

次の例では、レイヤ 2 アクセス ポートで IP デバイス トラッキング パラメータを設定する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```

ip device tracking probe

Address Resolution Protocol（ARP）プローブの IP デバイス トラッキング テーブルを設定するには、グローバル コンフィギュレーション モードで **ip device tracking probe** コマンドを使用します。ARP インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip device tracking probe {**count** *number*| **delay** *seconds*| **interval** *seconds*| **use-svi** *address*}

no ip device tracking probe {**count** *number*| **delay** *seconds*| **interval** *seconds*| **use-svi** *address*}

構文の説明

count*number*	デバイスが ARP プローブを送信する回数を設定します。範囲は 1 ～ 255 です。
delay*seconds*	デバイスが ARP プローブを送信するまで待機する秒数を設定します。指定できる範囲は 1 ～ 120 です。
interval*seconds*	デバイスが応答を待ち、ARP プローブを再送信するまでの秒数を設定します。指定できる範囲は 30 ～ 1814400 秒です。
use-svi	スイッチ仮想インターフェイス（SVI）IP アドレスを ARP プローブのソースとして使用します。

コマンド デフォルト

カウント番号は 3 です。

遅延はありません。

30 秒間隔です。

ARP プローブのデフォルト ソース IP アドレスはレイヤ 3 インターフェイスで、スイッチポートでは 0.0.0.0 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 ポートのデフォルト ソース IP アドレス 0.0.0.0 が使用され、ARP プローブがドロップする場合に、IP デバイス トラッキング テーブルが SVI IP アドレスを ARP プローブに使用するように設定するには、**use-svi** キーワードを使用します。

次の例では、SVI を ARP プローブのソースとして設定する方法を示します。

```
Device(config)# ip device tracking probe use-svi
```

ip dhcp snooping database

Dynamic Host Configuration Protocol（DHCP）のスヌーピング データベースを設定するには、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。DHCP スヌーピング サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping database {**crashinfo:***url* | **flash:***url* | **ftp:***url* | **http:***url* | **https:***url* | **rcp:***url* | **scp:***url* | **tftp:***url* | **timeout** *seconds* | **usbflash0:***url* | **write-delay** *seconds*}

no ip dhcp snooping database [**timeout**| **write-delay**]

構文の説明

crashinfo:*url*	crashinfo を使用して、エントリを格納するためのデータベースの URL を指定します。
flash:*url*	flash を使用して、エントリを格納するためのデータベースの URL を指定します。
ftp:*url*	FTP を使用して、エントリを格納するためのデータベースの URL を指定します。
http:*url*	HTTP を使用して、エントリを格納するためのデータベースの URL を指定します。
https:*url*	セキュア HTTP（HTTPS）を使用して、エントリを格納するためのデータベースの URL を指定します。

rcp:*url*	リモートコピー（RCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
scp:*url*	セキュアコピー（SCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
tftp:*url*	TFTP を使用して、エントリを格納するためのデータベースの URL を指定します。
timeout *seconds*	中断タイムアウトインターバルを指定します。有効値は 0 ～ 86,400 秒です。
usbflash0:*url*	USB flash を使用して、エントリを格納するためのデータベースの URL を指定します。
write-delay *seconds*	ローカル DHCP スヌーピングデータベースにデータが追加されてから、DHCP スヌーピングエントリを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ～ 86,400 秒です。

コマンド デフォルト

DHCP スヌーピング データベー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
Cisco IOS XE 3.2SE	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、インターフェイス上で DHCP スヌーピングをイネーブルにする必要があります。DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping** コマンドを使用します。

次に、TFTP を使用してデータベースの URL を指定する例を示します。

```
Device(config)#  ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

次に、DHCP スヌーピング エントリを外部サーバに書き込むまでの時間を指定する例を示します。

```
Device(config)#  ip dhcp snooping database write-delay 15
```

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、スイッチのグローバル 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 {**hostname** | **string** *string*}

no ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

構文の説明

hostname	スイッチのホスト名をリモート ID として指定します。
string *string*	1 ～ 63 の ASCII 文字（スペースなし）を使用して、リモート ID を指定します。

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
Cisco IOS XE 3.2SE	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。

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。

```
Device(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

DHCP クライアント メッセージのリレー エージェント アドレス（giaddr）が信頼できないポート上のクライアント ハードウェア アドレスに一致することを確認して、DHCP スヌーピング機能をディセーブルにするには、グローバル コンフィギュレーション モードで **ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証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。

ip dhcp snooping verify no-relay-agent-address

no ip dhcp snooping verify no-relay-agent-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

DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレー エージェント IP アドレス（giaddr）フィールドが 0 であることを確認します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレー エージェントの IP アドレス（giaddr）フィールドが 0 であることを確認します。giaddr フィールドが 0 でない場合、メッセージはドロップされます。検証をディセーブルにするには、**ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証を再度イネーブルにするには、**no ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。

次に、DHCP クライアント メッセージの giaddr 検証をイネーブルにする例を示します。

```
Device(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip http access-class

HTTP サーバへのアクセスを制限するために使用するアクセス リストを指定するには、グローバル コンフィギュレーション モードで **iphttpaccess-class** コマンドを使用します。以前に設定したアクセス リストの関連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。

（注） 既存の **ip http access-class***access-list-number* コマンドは、現在サポートされていますが、廃止される予定です。代わりに **ip http access-class ipv4** { *access-list-number* | *access-list-name* } and **ip http access-class ipv6***access-list-name* を使用します。

ip http access-class { *access-list-number* | **ipv4** { *access-list-number* | *access-list-name* } | **ipv6** *access-list-name* }

no ip http access-class { *access-list-number* | **ipv4** { *access-list-number* | *access-list-name* } | **ipv6** *access-list-name* }

構文の説明

ipv4	セキュア HTTP サーバへのアクセスを制限するように IPv4 アクセス リストを指定します。
ipv6	セキュア HTTP サーバへのアクセスを制限するように IPv6 アクセス リストを指定します。

access-list-number	グローバル コンフィギュレーション コマンド **access-list** を使用して設定される、0～99 の標準 IP アクセス リスト番号。
access-list-name	**ip access-list** コマンドで設定された標準 IPv4 アクセス リストの名前。

コマンド デフォルト

アクセス リストは、HTTP サーバには適用されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが変更されました。**ipv4** および **ipv6** キーワードが追加されました。
Cisco IOS XE Release 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドが設定されていると、指定されたアクセス リストは HTTP サーバに割り当てられます。HTTP サーバは、接続を受け入れる前にアクセス リストを確認します。確認に失敗すると、HTTP サーバは接続要求を承認しません。

次に、アクセス リストを 20 に定義して、HTTP サーバに割り当てる例を示します。

```
Device(config)# ip access-list standard 20
Device(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Device(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Device(config-std-nacl)# permit 209.165.200.225 0.255.255.255
Device(config-std-nacl)# exit
Device(config)# ip http access-class 20
```

次に、IPv4 の指定済みアクセス リストを定義して、HTTP サーバに割り当てる例を示します。

```
Device(config)# ip access-list standard Internet_filter
Device(config-std-nacl)# permit 1.2.3.4
Device(config-std-nacl)# exit
```

```
Device(config)# ip http access-class ipv4 Internet_filter
```

関連コマンド

コマンド	説明
ipaccess-list	ID をアクセス リストに割り当て、アクセス リストのコンフィギュレーション モードを開始します。
iphttpserver	HTTP 1.1 サーバ（Cisco Web ブラウザ ユーザ インターフェイスを含む）をイネーブルにします。

ip source binding

スタティック IP ソース バインディング エントリを追加するには、**ip source binding** コマンドを使用します。スタティック IP ソース バインディング 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 source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

no ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	バインディング対象 MAC アドレスです。
vlan *vlan-id*	レイヤ 2 VLAN ID を指定します。有効な値は 1～4094 です。
ip-address	バインディング対象 IP アドレスです。
interface *interface-id*	物理インターフェイスの ID です。

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
Cisco IOS XE 3.2SE	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、スタティック IP ソース バインディング エントリだけを追加するために使用できます。

no 形式は、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるためには、すべての必須パラメータが正確に一致しなければなりません。各スタティック IP バインディング エントリは MAC アドレスと VLAN 番号がキーであることに注意してください。コマンドに既存の MAC アドレスと VLAN 番号が含まれる場合、別のバインディング エントリが作成される代わりに既存のバインディング エントリが新しいパラメータで更新されます。

次の例では、スタティック IP ソース バインディング エントリを追加する方法を示します。

```
Device# configure terminal
Deviceconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
```

ip verify source

インターフェイス上の 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 [**mac-check**][**tracking**]

no ip verify source

構文の説明

mac-check	（任意）MAC アドレス検証による IP ソース ガードをイネーブルにします。
tracking	（任意）ポートで静的 IP アドレス を学習するために IP ポート セキュリティをイネーブルにします。

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
Cisco IOS XE 3.2SE	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 アドレス フィルタリングおよび MAC アドレス検証による IP ソース ガードをイネーブルにするには、**ip verify sourcemac-check** インターフェイス コンフィギュレーション コマンドを使用します。

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 ガードをインターフェイス上でイネーブルにする方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

次の例では、MAC アドレスの検証による IP ソース ガードをイネーブルにする方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source mac-check

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip dhcp snooping
Device(config)# ip dhcp snooping vlan 10 20
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport trunk encapsulation dot1q
Device(config-if)# switchport mode trunk
Device(config-if)# switchport trunk native vlan 10
Device(config-if)# switchport trunk allowed vlan 11-20
Device(config-if)# no ip dhcp snooping trust
Device(config-if)# ip verify source vlan dhcp-snooping
Device(config)# end
Device# show ip verify source interface fastethernet0/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Gi1/0/1      ip-mac       active       10.0.0.1                          10
Gi1/0/1      ip-mac       active       deny-all                          11-20
Device#


Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# ip verify source tracking port-security
Device(config-if)# end
```

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

ipv6 access-list

IPv6 アクセス リストを定義してデバイスを IPv6 アクセス リスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6access-list** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*

noipv6 access-list *access-list-name* | **client** *permit-control-packets*| **log-update** *threshold* | **role-based** *list-name*

構文の説明

ipv6 *access-list-name*	名前付き IPv6 ACL（最長 64 文字）を作成し、IPv6 ACL コンフィギュレーション モードを開始します。 *access-list-name*：IPv6 アクセス リストの名前。名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。
match-local-traffic	ローカルで生成されたトラフィックに対する照合を有効にします。
log-update threshold *threshold-in-msgs*	最初のパケットの一致後に、syslog メッセージを生成する方法を決定します。 *threshold-in-msgs*：生成されるパケット数。
role-based *list-name*	ロールベースの IPv6 ACL を作成します。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドは Cisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

使用上のガイドライン

IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6access-list** コマンドを使用することで定義され、その許可と拒否の条件は IPv6 アクセス リスト コンフィギュレーション モードで **deny** および **permit** コマンドを使用することで設定されます。**ipv6access-list** コマンドを設定すると、デバイスは IPv6 アクセス リスト コンフィギュレーション モードになり、デバイス プロンプトは Device(config-ipv6-acl)# に変わります。IPv6 アクセス リスト コンフィギュレーション モードから、定義済みの IPv6 ACL に許可および拒否の条件を設定できます。

（注） IPv6 ACL は一意な名前によって定義されます（IPv6 は番号付けされた ACL をサポートしません）。IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permitanyany** ステートメントおよび **denyanyany** ステートメントでプロトコル タイプとして自動的に設定されます。

すべての IPv6 ACL には、最終一致条件として、暗黙の **permiticmpanyanynd-na**、**permiticmpanyanynd-ns** および **denyipv6anyany** の各ステートメントがあります（前の 2 つの一致条件は、ICMPv6 ネイバー探索を許可します）。1 つの IPv6 ACL には、暗黙の **denyipv6anyany** ステートメントを有効にするために少なくとも 1 つのエントリが含まれている必要があります。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

IPv6 ACL を IPv6 インターフェイスに適用するには、*access-list-name* 引数を指定して **ipv6traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ACL をデバイスとの着信および発信 IPv6 仮想端末接続に適用するには、*access-list-name* 引数を指定して、**ipv6access-class** ライン コンフィギュレーション コマンドを使用します。

ipv6traffic-filter コマンドでインターフェイスに適用される IPv6 ACL は、デバイスによって発信されたトラフィックではなく、転送されたトラフィックをフィルタ処理します。

次に、list1 という名前の IPv6 ACL を設定し、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

次に、list2 という名前の IPv6 ACL を設定し、その ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用する例を示します。特に、最初の ACL エントリは、ネットワーク FEC0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィックス FEC0:0:0:2 を持つパケット）がイーサネットインターフェイス0から出て行くことを拒否します。2 番目の ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。2 番目のエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

ipv6 snooping policy

（注） すべての既存の IPv6 スヌーピング コマンド（Cisco IOS XE Denali 16.1.1 より前）には、対応する SISF ベースのデバイス トラッキング コマンドが用意され、IPv4 と IPv6 の両方のアドレス ファミリに設定を適用できるようになりました。詳細については、「device-tracking policy」を参照してください。

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 snooping policy** コマンドを使用します。IPv6 スヌーピング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy *snooping-policy*

no ipv6 snooping policy *snooping-policy*

構文の説明

snooping-policy	スヌーピング ポリシーのユーザ定義名。ポリシー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

IPv6 スヌーピング ポリシー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
Cisco IOS XE 3.2SE	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 スヌーピング ポリシーを作成するには、**ipv6 snooping policy** コマンドを使用します。**ipv6 snooping policy** コマンドがイネーブルの場合、コンフィギュレーション モードが IPv6 スヌーピング コンフィギュレーション モードに変更されます。このモードでは、管理者が次の IPv6 ファーストホップ セキュリティ コマンドを設定できます。

- **device-role** コマンドは、ポートに接続されているデバイスのロールを指定します。
- **limit address-count** *maximum* コマンドは、ポートで使用できる IPv6 アドレスの数を制限します。
- **protocol** コマンドは、アドレスを Dynamic Host Configuration Protocol（DHCP）または Neighbor Discovery Protocol（NDP）で収集する必要があることを指定します。
- **security-level** コマンドは、適用されるセキュリティのレベルを指定します。
- **tracking** コマンドは、ポートのデフォルトのトラッキング ポリシーに優先します。
- **trusted-port** コマンドは、ポートを信頼できるポートとして設定します。つまり、メッセージを受信したときに検証が限定的に実行されるか、まったく実行されません。

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)#
```

key chain macsec

事前共有キー（PSK）を取得するためにデバイス インターフェイスの MACsec キー チェーンの名前を設定するには、グローバル コンフィギュレーション モードで **key chain macsec** コマンドを使用します。CDP 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。

key chain *name***macsec** {**description**| **key**| **exit**}

構文の説明

name	キーを取得するために使用するキー チェーンの名前。
description	MACsec キー チェーンの説明を入力します。

key	MACsec キーを設定します。
exit	MACsec キーチェーン 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、またはデフォルト値を設定します。

コマンド デフォルト

key chain macsec は無効になっています。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

次に、128 ビットの事前共有キー（PSK）を取得するために MACsec キー チェーンを設定する例を示します。

```
Switch#configure terminal
Switch(config)#key chain kc1 macsec
Switch(config-keychain-macsec)#key 1000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-128-cmac
Switch(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Switch(config-keychain-macsec-key)#end
Switch#
```

次に、256 ビットの事前共有キー（PSK）を取得するために MACsec キー チェーンを設定する例を示します。

```
Switch#configure terminal
Switch(config)#key chain kc1 macsec
Switch(config-keychain-macsec)#key 2000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-256-cmac
Switch(config-keychain-macsec-key)# key-string
c865632acb269022447c417504a1bf5db1c296449b52627ba01f2ba2574c2878
Switch(config-keychain-macsec-key)#end
Switch#
```

limit address-count

ポートで使用できる IPv6 アドレスの数を制限するには、Neighbor Discovery Protocol（NDP）インスペクション ポリシー コンフィギュレーション モードまたは IPv6 スヌーピング コンフィギュレーション モードで **limit address-count** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

limit address-count *maximum*

no limit address-count

構文の説明

maximum	ポートで許可されているアドレスの数。範囲は 1 ～ 10000 です。

コマンド デフォルト

デフォルト設定は無制限です。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

limit address-count コマンドは、ポリシーが適用されているポートで使用できる IPv6 アドレスの数を制限します。ポート上の IPv6 アドレスの数を制限すると、バインディング テーブル サイズの制限に役立ちます。範囲は 1 ～ 10000 です。

次に、NDP ポリシー名を policy1 と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
```

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
```

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 vlan access-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。

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
Cisco IOS XE 3.2SE	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機能を使用します。Cisco ACS はこのコマンドを無視します。

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。

```
Device(config)# mab request format attribute 32 vlan access-vlan
```

関連コマンド

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

macsec network-link

アップリンク インターフェイスの MKA MACsec 設定を有効にするには、インターフェイスで **macsec network-link** コマンドを使用します。CDP 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。

macsec network-link

構文の説明

macsec network-link	EAP-TLS 認証プロトコルを使用してデバイス インターフェイスの MKA MACsec 設定を有効にします。

コマンド デフォルト

macsec network-link は無効になっています。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

次に、EAP-TLS 認証プロトコルを使用して、インターフェイスに MACsec MKA を設定する例を示します。

```
Switch#configure terminal
Switch(config)# int G1/0/20
Switch(config-if)# macsec network-link
Switch(config-if)# end
Switch#
```

match（アクセス マップ コンフィギュレーション）

1 つまたは複数のアクセス リストをパケットと照合するように VLAN マップを設定するには、スイッチ スタックまたはスタンドアロン スイッチのアクセスマップ 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。照合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*]...| **ipv6 address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **ipv6 address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

構文の説明

ip address	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
ipv6 address	パケットを IPv6 アドレス アクセス リストと照合するようにアクセス マップを設定します。
mac address	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
name	パケットを照合するアクセス リストの名前です。
number	パケットを照合するアクセス リストの番号です。このオプションは、MAC アクセス リストに対しては無効です。

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
Cisco IOS XE 3.2SE	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、IPv6 パケットは IPv6 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、IPv6 アドレスおよび MAC アドレスを指定できます。

次の例では、VLAN アクセス マップ vmap4 を定義して VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップでは、パケットがアクセス リスト al2 に定義された条件に一致すると、インターフェイスは IP パケットをドロップします。

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(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。

関連トピック

action, （1027 ページ）

show vlan access-map, （1131 ページ）

vlan access-map, （1161 ページ）

mka pre-shared-key

事前共有キー（PSK）を使用してデバイス インターフェイスの MKA MACsec 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 **mka pre-shared-key key-chain***key-chain name* コマンドを使用します。CDP 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。

mka pre-shared-key key-chain *key-chain-name*

構文の説明

mka pre-shared-key key-chain	PSK を使用してデバイス インターフェイスの MACsec MKA 設定を有効にします。

コマンド デフォルト

mka pre-shared-key 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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

次に、PSK を使用して、インターフェイスの MKA MACsec を設定する例を示します。

```
Switch#
Switch(config)# int G1/0/20
Switch(config-if)# mka pre-shared-key key-chain kc1
Switch(config-if)# end
Switch#
```

no authentication logging verbose

認証システム メッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **no authentication logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

no authentication logging verbose

構文の説明

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

すべての詳細情報はシステム メッセージに表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、認証システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 認証システム メッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# no authentication logging verbose
```

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

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC 認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

no dot1x logging verbose

802.1x システム メッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチのグローバル コンフィギュレーション モードで **no dot1x logging verbose** コマンドを使用します。

no dot1x logging verbose

構文の説明

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

すべての詳細情報はシステム メッセージに表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、802.1x システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 802.1x システム メッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# no dot1x logging verbose
```

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

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC 認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

no mab logging verbose

MAC 認証バイパス（MAB）のシステム メッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **no mab logging verbose** コマンドを使用します。

no mab logging verbose

構文の説明

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

すべての詳細情報はシステム メッセージに表示されます。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、MAC 認証バイパス（MAB）システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose MAB システム メッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# no mab logging verbose
```

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

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

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、スイッチスタックまたはスタンドアロン スイッチ上で **permit** MAC アクセスリスト コンフィギュレーション コマンドを使用します。拡張 MAC アクセス リストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

{**permit** {**any** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **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**][**cos***cos*]

nopermit {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **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**][**cos***cos*]

構文の説明

any	すべての送信元または宛先 MAC アドレスを拒否します。
host*src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを指定します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを指定します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	（任意）パケットの EtherType 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。 • *type* には、0 ～ 65535 の 16 進数を指定できます。 • *mask* は、一致をテストする前に EtherType に適用される don't care ビットのマスクです。
aarp	（任意）データリンクアドレスをネットワークアドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。
amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを指定します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	（任意）EtherType DEC-Diagnostic を指定します。
dsm	（任意）EtherType DEC-DSM を指定します。
etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。

lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します。
lsap*lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を指定します。
mop-dump	（任意）EtherType DEC-MOP Dump を指定します。
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NetBIOS）を指定します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を指定します。
vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）EtherType Xerox Network Systems（XNS）プロトコル スイートを指定します。
cos*cos*	（任意）プライオリティを設定するため、0 ～ 7 までの任意の Class of Service（CoS）値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

appletalk は、コマンドラインのヘルプ ストリングには表示されますが、一致条件としてはサポートされていません。

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

host キーワードを使用した場合、アドレス マスクは入力できません。 **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）がアクセス コントロール リストに追加されると、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。

IPX トラフィックをフィルタ処理するには、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。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、次の表に一覧表示します。

表 *40* : *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

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。

```
Device(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。

```
Device(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。

```
Device(config-ext-macl)# permit any any 0x4321 0
```

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

関連コマンド

コマンド	説明
deny	MAC アクセスリスト コンフィギュレーションを拒否します。条件が一致した場合に非 IP トラフィックが転送されるのを拒否します。
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

propagate sgt (cts manual)

Cisco TrustSec Security（CTS）インターフェイスでレイヤ 2 のセキュリティ グループ タグ（SGT）伝達を有効にするには、インターフェイス コンフィギュレーション モードで **propagate sgt** コマンドを使用します。SGT 伝達を無効にするには、このコマンドの **no** 形式を使用します。

propagate sgt

構文の説明

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

SGT 処理の伝達が有効になっています。

コマンド モード

CTS 手動インターフェイス コンフィギュレーション モード（config-if-cts-manual）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

SGT 処理の伝達によって、CTS 対応のインターフェイスは L2 SGT タグに基づいて CTS メタ データ（CMD）を受信および送信できます。ピア デバイスが SGT を受信できず、その結果、SGT タグを L2 ヘッダーに配置できない状況で、インターフェイスの SGT 伝達を無効にするには **no propagate sgt** コマンドを使用します。

次に、手動で設定された TrustSec 対応のインターフェイスで SGT 伝達を無効にする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# no propagate sgt
```

次に、ギガビット イーサネット インターフェイス 0 で SGT 伝達が無効になっている例を示します。

```
Switch#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Disabled
    Cache Info:
        Cache applied to link : NONE
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
show cts interface	インターフェイスごとの Cisco TrustSec ステートおよび統計情報を表示します。

protocol（IPv6 スヌーピング）

アドレスを Dynamic Host Configuration Protocol（DHCP）または Neighbor Discovery Protocol（NDP）で収集する必要があることを指定するか、プロトコルを IPv6 プレフィックス リストに対応させるには、**protocol** コマンドを使用します。DHCP または NDP によるアドレス収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol {**dhcp** | **ndp**}

no protocol {**dhcp** | **ndp**}

構文の説明

dhcp	アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）パケットで収集する必要があることを指定します。
ndp	アドレスをネイバー探索プロトコル（NDP）パケットで収集する必要があることを指定します。

コマンド デフォルト

スヌーピングとリカバリは DHCP および NDP の両方を使用して試行します。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

アドレスが DHCP または NDP に対応するプレフィックス リストと一致しない場合は、制御パケットがドロップされ、バインディング テーブル エントリのリカバリはそのプロトコルに対しては試行されません。

- **no protocol** {**dhcp** | **ndp**} コマンドを使用すると、プロトコルはスヌーピングまたはグリーニングに使用されません。
- **no protocol dhcp** コマンドを使用すると、DHCP は依然としてバインディング テーブルのリカバリに使用できます。

- データ収集は DHCP および NDP でリカバリできますが、宛先ガードは DHCP によってのみリカバリできます。

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、アドレスの収集に DHCP を使用するようにポートを設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
```

sap mode-list (cts manual)

2 個のインターフェイスの間のリンク暗号化をネゴシエートするために使用される Security Association Protocol（SAP）の認証と暗号化モード（最高から最低に優先順位付けされた）を選択するには、CTS dot1x インターフェイス コンフィギュレーション モードで **sap mode-list** コマンドを使用します。モードリストを削除して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。

2 個のインターフェイス間で MACsec のリンク暗号化をネゴシエートするために、ペアワイズ マスター キー（PMK）と Security Association Protocol（SAP）の認証および暗号化モードを手動で指定するには、**sap mode-list** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

sap pmk mode-list {**gcm-encrypt**| **gmac**| **no-encap**| **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

no sap pmk mode-list {**gcm-encrypt**| **gmac**| **no-encap**| **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

構文の説明

pmk*hex_value*	16 進数データ PMK を指定します（先行する 0x なし。偶数の 16 進数文字を入力する。そうでない場合は、最後の文字に 0 のプレフィックスが付加される）。
mode-list	アドバタイズされたモードのリストを指定します（最高から最低に優先順位付け）。
gcm-encrypt	GMAC 認証、GCM 暗号化を指定します。
gmac	GMAC 認証だけを指定し、暗号化を指定しません。
no-encap	カプセル化を指定しません。

null	カプセル化あり、認証なし、暗号化なしを指定します。

コマンド デフォルト

デフォルトのカプセル化は、**sap pmk mode-list gcm-encrypt null** です。ピア インターフェイスが 802.1AE MACsec または 802.REV レイヤ 2 リンク暗号化をサポートしない場合、デフォルトの暗号化は **null** です。

コマンド モード

CTS 手動インターフェイス コンフィギュレーション（config-if-cts-manual）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

認証と暗号化方式を指定するには、**sap pmk mode-list** コマンドを使用します。

セキュリティ アソシエーション プロトコル（SAP）は 802.11i IEEE プロトコルのドラフト バージョンに基づいた暗号キーの取得および交換プロトコルです。SAP は MACsec をサポートするインターフェイス間の 802.1AE リンク間暗号化（MACsec）を確立および管理するために使用します。

SAP およびペアワイズ マスター キー（PMK）は、**sap pmk mode-list** コマンドを使用して、2 個のインターフェイス間に手動で設定することもできます。802.1X 認証を使用する場合、両方（サプリカントおよびオーセンティケータ）が Cisco Secure Access Control Server からピアのポートの PMK および MAC アドレスを受信します。

デバイスが CTS 対応ソフトウェアを実行していて、ハードウェアが CTS 非対応である場合は、**sap mode-list no-encap** コマンドを使用してカプセル化を拒否します。

次に、ギガビット イーサネット インターフェイスで SAP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk FFFEE mode-list gcm-encrypt
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
propagate sgt (cts manual)	Cisco TrustSec Security（CTS）のレイヤ 2 でのセキュリティ グループ タグ（SGT）伝達を有効にします。
show cts interface	Cisco TrustSec インターフェイス設定の統計情報を表示します。

security level（IPv6 スヌーピング）

適用されるセキュリティのレベルを指定するには、IPv6 スヌーピング ポリシー コンフィギュレーション モードで **security-level** コマンドを使用します。

security level {**glean** | **guard** | **inspect**}

構文の説明

glean	アドレスをメッセージから抽出し、検証を行わずにそれらをバインディング テーブルにインストールします。
guard	収集と検査の両方を実行します。さらに、信頼できるポートで受信されていない場合、または別のポリシーによって許可されていない場合、RA メッセージおよび DHCP サーバ メッセージは拒否されます。
inspect	メッセージの一貫性と準拠度を検証します。特に、アドレス所有権が強制されます。無効なメッセージはドロップされます。

コマンド デフォルト

デフォルトのセキュリティ レベルは guard です。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、セキュリティ レベルを inspect として設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
```

security passthru

IPSec のパススルーを変更するには、**securitypassthru** コマンドを使用します。ディセーブルにするには、このコマンドの no 形式を使用します。

security passthru *ip-address*

no security passthru

構文の説明

ip-address	（任意）VPN トンネルの終端となる IPSec ゲートウェイ（ルータ）の IP アドレスです。

コマンド デフォルト

なし。

コマンド モード

wlan

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、IPSec のパススルーを変更する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#security passthrough 10.1.1.1
```

show aaa clients

AAA クライアントの統計情報を表示するには、**show aaa clients** コマンドを使用します。

show aaa clients [**detailed**]

構文の説明

detailed	（任意）詳細な AAA クライアントの統計情報を示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show aaa clients** コマンドの出力を示します。

```
Device# show aaa clients

Dropped request packets: 0
```

show aaa command handler

AAA コマンド ハンドラの統計情報を表示するには、**show aaa command handler** コマンドを使用します。

show aaa command handler

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show aaa command handler** コマンドの出力を示します。

```
Device# show aaa command handler

AAA Command Handler Statistics:
    account-logon: 0, account-logoff: 0
    account-query: 0, pod: 0
    service-logon: 0, service-logoff: 0
    user-profile-push: 0, session-state-log: 0
    reauthenticate: 0, bounce-host-port: 0
    disable-host-port: 0, update-rbacl: 0
    update-sgt: 0, update-cts-policies: 0
    invalid commands: 0
    async message not sent: 0
```

show aaa local

AAA ローカル方式オプションを表示するには、**show aaa local** コマンドを使用します。

show aaa local {**netuser**{*name* | **all**} |**statistics** | **user lockout**}

構文の説明

netuser	AAA ローカル ネットワークまたはゲスト ユーザ データベースを指定します。
name	ネットワーク ユーザ名。
all	ネットワークおよびゲスト ユーザ情報を指定します。
statistics	ローカル認証の統計情報を表示します。
user lockout	AAA ローカルのロックアウトされたユーザを指定します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show aaa local statistics** コマンドの出力を示します。

```
Device# show aaa local statistics

Local EAP statistics

EAP Method         Success       Fail
---------------------------------------
Unknown                  0          0
EAP-MD5                  0          0
EAP-GTC                  0          0
LEAP                     0          0
PEAP                     0          0
EAP-TLS                  0          0
EAP-MSCHAPV2             0          0
EAP-FAST                 0          0

Requests received from AAA:                  0
Responses returned from EAP:                 0
Requests dropped (no EAP AVP):               0
Requests dropped (other reasons):            0
Authentication timeouts from EAP:            0

Credential request statistics
Requests sent to backend:                    0
Requests failed (unable to send):            0
Authorization results received

  Success:                                   0
  Fail:                                      0
```

show aaa servers

AAA サーバの MIB によって認識されるすべての AAA サーバを表示するには、**show aaa servers** コマンドを使用します。

show aaa servers [**private**|**public**|[**detailed**]]

構文の説明

detailed	（任意）AAA サーバの MIB によって認識されるプライベート AAA サーバを表示します。
public	（任意）AAA サーバの MIB によって認識されるパブリック AAA サーバを表示します。
detailed	（任意）詳細な AAA サーバの統計情報を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show aaa servers** コマンドの出力を示します。

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

AAA セッション MIB によって認識される AAA セッションを表示するには、**show aaa sessions** コマンドを使用します。

show aaa sessions

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show aaa sessions** コマンドの出力を示します。

```
Device# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
   Unique Id: 4025
   User Name: *not available*
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
```

show authentication history

デバイスで稼働中の認証セッションを表示するには、**show authentication history** コマンドを使用します。

show authentication history [**min-uptime** *seconds*]

構文の説明

min-uptime *seconds*	（任意）最小アップタイム内のセッションを表示します。有効範囲は 1 ～ 4294967295 秒です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デバイスで稼働中の認証セッションを表示するには、**show authentication history** コマンドを使用します。

次の例では、**show authentication history** コマンドの出力を示します。

```
Device# show authentication history
Interface  MAC Address     Method  Domain  Status  Uptime
Gi3/0/2    0021.d864.07c0  dot1x   DATA    Auth    38s

Session count = 1
```

show authentication sessions

現在の認証マネージャ セッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。

show authentication sessions [**database**][**handle***handle-id*[**details**]][**interface** *type number*[**details**][**mac** *mac-address*[**interface** *type number*][**method** *method-name*[**interface** *type number*[**details**] [**session-id** *session-id* [**details**]]

構文の説明

database	（任意）セッション データベースに格納されているデータだけを示します。
handle*handle-id*	（任意）認証マネージャ情報を表示する特定のハンドルを指定します。
details	（任意）詳細情報を表示します。
interface*typenumber*	（任意）認証マネージャ情報を表示する特定のインターフェイスのタイプと番号を指定します。
mac*mac-address*	（任意）情報を表示する特定の MAC アドレスを指定します。
method*method-name*	（任意）認証マネージャ情報を表示する特定の認証方法を指定します。方式を指定する場合（**dot1x**、**mab**、または **webauth**）、インターフェイスも指定できます。
session-id*session-id*	（任意）認証マネージャ情報を表示する特定のセッションを指定します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

現在のすべての認証マネージャ セッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。特定の認証マネージャ セッションに関する情報を表示するには、1 つ以上のキーワードを使用します。

このテーブルは、報告された認証セッションで想定される動作状態を示します。

表 *41*：認証方式のステート

状態	説明
Not run	このセッションの方式は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。
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。
Success	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	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。

次の表に、使用できる認証方式を示します。

表 *42*：認証方式のステート

状態	説明
dot1x	802.1X
mab	MAC 認証バイパス
webauth	Web 認証

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions
Interface    MAC Address     Method   Domain   Status         Session ID
Gi1/0/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/0/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/0/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions interface gigabitethernet2/0/47
            Interface:  GigabitEthernet2/0/47
          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:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C80000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
            Interface:  GigabitEthernet2/0/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C80000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

show cts interface

インターフェイスの Cisco TrustSec（CTS）設定の統計を表示するには、特権 EXEC モードで **show cts interface** コマンドを使用します。

show cts interface [**type** *slot/port*| **brief**| **summary**]

構文の説明

type*slot/port*	（任意）インターフェイスタイプおよびスロット番号またはポート番号を指定します。このインターフェイスの詳細な出力が返されます。
brief	（任意）すべてのCTSインターフェイスの短縮ステータスを表示します。
summary	（任意）インターフェイスごとに、すべてのCTS インターフェイスのサマリーを、4 個または 5 個のキー ステータス フィールドを持つ表形式で表示します。

コマンド デフォルト

なし

コマンド モード

EXEC（>） 特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが変更され、いくつかのオプションが追加されました。
Cisco IOS XE Denali 16.2.1	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CTSインターフェイスの冗長ステータスを表示するには、キーワードを使用せずに**show cts interface** コマンドを使用します。

次に、キーワードを使用せずに出力を表示する例を示します（すべてのCTSインターフェイスの冗長ステータス）。

```
Switch# show cts interface

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
```

```
    Interface Active for 00:00:18.232
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:

    Propagate SGT:           Enabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0
```

次に、**brief** キーワードを使用した出力例を示します。

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Interface Active for 00:00:40.386
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Cache applied to link : NONE
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
propagate sgt (cts manual)	Cisco TrustSec Security（CTS）インターフェイスのレイヤ 2 でのセキュリティ グループ タグ（SGT）の伝達を有効にします。
sap mode-list (cts manual)	PMK および SAP 認証モードと暗号化モードを手動で指定し、2 つのインターフェイス間で MACsec リンクの暗号化をネゴシエートします。

show cts role-based permissions

ロールベース（セキュリティ グループ）アクセス コントロール権限リストを表示するには、特権 EXEC モードで **show cts role-based permissions** コマンドを使用します。

show cts role-based permissions[**default**[**details**| **ipv4**[**details**]] | **from**[*sgt*[**ipv4**| **～**[*sgt*| **unknown**] [**details**| **ipv4**[**details**]]] | **unknown**] | **ipv4**| **to**[*sgt*| **unknown**] [**ipv4**]]

構文の説明

default	（任意）デフォルトの権限リストに関する情報を表示します。
details	（任意）アタッチされたアクセス コントロール リスト（ACL）の詳細を表示します。
ipv4	（任意）IPv4 プロトコルに関する情報を表示します。
from	（任意）送信元グループに関する情報を表示します。
sgt	（任意）セキュリティ グループ タグ。有効値は 2 ～ 65519 です。
to	（任意）宛先グループに関する情報を表示します。
unknown	（任意）不明な送信元グループと宛先グループに関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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、SGACL 権限マトリックスのコンテンツを表示します。送信元セキュリティ グループ タグ（SGT）は **from** キーワードを使用して、宛先 SGT は **to** キーワードを使用して指定できます。両方のキーワードを指定すると、単一セルの RBACL が表示されます。列全体は、**to** キーワードを使用した場合にのみ表示されます。行全体は、**from** キーワードを使用した場合にのみ表示されます。権限マトリックス全体は、**from** キーワードと **to** キーワードの両方を省略した場合に表示されます。

コマンド出力は、プライマリ キーの宛先 SGT およびセカンダリ キーの送信元 SGT でソートされます。各セルの SGACL は、設定で定義されているのと同じ順序で、または Cisco Identity Services Engine（ISE）から取得した順序で表示されます。

details キーワードは、**from** キーワードと **to** キーワードの両方を指定することで、単一のセルが選択された場合に表示されます。**details** キーワードが指定されている場合、単一セルの SGACL のアクセス制御エントリが表示されます。

次に、**show role-based permissions** コマンドの出力例を示します。

```
Switch# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):
  mon_1
IPv4 Role-based permissions from group 10 to group 11 (configured):
  mon_2
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

関連コマンド

コマンド	説明
cts role-based permissions	送信元グループから宛先グループに対する権限を有効にします。
cts role-based monitor	ロールベースのアクセス リストのモニタリングを有効にします。

show cisp

指定されたインターフェイスの CISP 情報を表示するには、**show cisp** 特権 EXEC コマンドを使用します。

show cisp {[**clients** | **interface** *interface-id*] | **registrations** | **summary**}

構文の説明

クライアント	（任意）CISP クライアントの詳細を表示します。
interface*interface-id*	（任意）指定されたインターフェイスの CISP 情報を表示します。有効なインターフェイスには、物理ポートとポートチャネルが含まれます。
registrations	CISP の登録情報を表示します。
summary	（任意）CISP のサマリー情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドは Cisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

次の例では、**show cisp interface** コマンドの出力を示します。

```
Device# show cisp interface fast 0
CISP not enabled on specified interface
```

次の例では、**show cisp registration** コマンドの出力を示します。

```
Device# show cisp registrations
```

```
Interface(s) with CISP registered user(s):
-----------------------------------------
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
dot1x credentials*profile*	サプリカント スイッチでプロファイルを設定します。

show dot1x

スイッチまたは指定されたポートのIEEE 802.1x統計情報、管理ステータス、および動作ステータスを表示するには、ユーザ EXEC モードで **show dot1x** コマンドを使用します。

show dot1x [**all** [**count**| **details**| **statistics**| **summary**]] [**interface***type number*[**details**| **statistics**]] [**statistics**]

構文の説明

all	（任意）すべてのインターフェイスのIEEE 802.1x情報を表示します。
count	（任意）許可されたクライアントと無許可のクライアントの総数を表示します。
details	（任意）IEEE 802.1xインターフェイスの詳細を表示します。
statistics	（任意）すべてのインターフェイスのIEEE 802.1x統計情報を表示します。

summary	（任意）すべてのインターフェイスの IEEE 802.1x サマリー情報を表示します。
interface*type number*	（任意）指定したポートの IEEE 802.1X ステータスを表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show dot1x all** コマンドの出力を示します。

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3
```

次の例では、**show dot1x all count** コマンドの出力を示します。

```
Device# show dot1x all count
Number of Dot1x sessions
------------------------------
Authorized Clients        = 0
UnAuthorized Clients      = 0
Total No of Client        = 0
```

次の例では、**show dot1x all statistics** コマンドの出力を示します。

```
Device# show dot1x statistics
Dot1x Global Statistics for
-------------------------------------------
RxStart = 0     RxLogoff = 0    RxResp = 0      RxRespID = 0
RxReq = 0       RxInvalid = 0   RxLenErr = 0
RxTotal = 0

TxStart = 0     TxLogoff = 0    TxResp = 0
TxReq = 0       ReTxReq = 0     ReTxReqFail = 0
TxReqID = 0     ReTxReqID = 0   ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

拡張認証プロトコル（EAP）のセキュア トンネリングを介したフレキシブル認証（FAST）ピアの格納済み Protected Access Credential（PAC）を表示するには、特権 EXEC モードで **show eap pac peer** コマンドを使用します。

show eap pac peer

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例は、**show eap pac peers** 特権 EXEC コマンドの出力を示します。

```
Device> show eap pac peers
No PACs stored
```

関連コマンド

コマンド	説明
clear eap sessions	スイッチまたは指定されたポートの EAP のセッション情報をクリアします。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報を概要形式または詳細形式で表示するには、ユーザ EXEC モードで **show ip dhcp snooping statistics** コマンドを使用します。

構文の説明

show ip dhcp snooping statistics [detail]

detail	（任意）詳細な統計情報を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。新しいアクティブ スイッチが選定された場合、統計カウンタはリセットされます。

次の例では、**show ip dhcp snooping statistics** コマンドの出力を示します。

```
Device> 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。

```
Device> 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
```

次の表に、DHCP スヌーピング統計情報およびその説明を示します。

表 *43* : *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。

DHCP スヌーピング統計情報	説明
Packets Dropped Because IDB not known	パケットの入力インターフェイスを判断できないエラーの数。
Queue full	パケットの処理に使用される内部キューが満杯であるエラーの数。非常に高いレートで DHCP パケットを受信し、入力ポートでレート制限がイネーブルになっていない場合、このエラーが発生することがあります。
Interface is in errdisabled	errdisable としてマークされたポートでパケットを受信した回数。これが発生する可能性があるのは、ポートが errdisable ステートである場合にパケットが処理キューに入り、そのパケットが後で処理される場合です。
Rate limit exceeded	ポートで設定されているレート制限を超えて、インターフェイスが errdisable ステートになった回数。
Received on untrusted ports	信頼できないポートで DHCP サーバ パケット（OFFER、ACK、NAK、LEASEQUERY のいずれか）を受信してドロップした回数。
Nonzero giaddr	信頼できないポートで受信した DHCP パケットのリレーエージェントアドレスフィールド（giaddr）がゼロ以外だった回数。または **no ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを設定しておらず、信頼できないポートで受信したパケットにオプション 82 データが含まれていた回数。
Source mac not equal to chaddr	DHCP パケットのクライアント MAC アドレス フィールド（chaddr）がパケットの送信元 MAC アドレスと一致せず、**ip dhcp snooping verify mac-address** グローバル コンフィギュレーション コマンドが設定されている回数。
Binding mismatch	MAC アドレスと VLAN のペアのバインディングになっているポートとは異なるポートで、RELEASE パケットまたは DECLINE パケットを受信した回数。これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがスイッチの別のポートに移動して RELEASE または DECLINE を実行したことを表すこともあります。MAC アドレスは、イーサネット ヘッダーの送信元 MAC アドレスではなく、DHCP パケットの chaddr フィールドから採用されます。

DHCP スヌーピング統計情報	説明
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。
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。

show radius server-group

RADIUS サーバ グループのプロパティを表示するには、**show radius server-group** コマンドを使用します。

show radius server-group {*name*| **all**}

構文の説明

name	サーバ グループの名前。サーバ グループの名前の指定に使用する文字列は、**the aaa group server radius** コマンドを使用して定義する必要があります。
all	すべてのサーバ グループのプロパティを表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

aaa group server radius コマンドで定義したサーバ グループを表示するには、**show radius server-group** コマンドを使用します。

次の例では、**show radius server-group all** コマンドの出力を示します。

```
Device# show radius server-group all
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *44* : *show radius server-groups* コマンドのフィールドの説明

フィールド	説明
Server group	サーバ グループの名前。
Sharecount	このサーバグループを共有している方式リストの数。たとえば、1つの方式リストが特定のサーバ グループを使用する場合、sharecount は 1 です。2 つの方式リストが同じサーバ グループを使用する場合、sharecount は 2 です。
sg_unconfigured	サーバ グループが設定解除されました。
Type	タイプは、standard または nonstandard のいずれかです。タイプはグループ内のサーバが非標準の属性を受け入れるかどうかを示します。グループ内のすべてのサーバに非標準のオプションが設定されている場合、タイプは「nonstandard」と表示されます。

フィールド	説明
Memlocks	メモリ内にあるサーバグループ構造の内部参照の数。この数は、このサーバグループへの参照を保持している内部データ構造パケットまたはトランザクションがいくつあるかを表します。Memlocks はメモリ管理のために内部的に使用されます。

show storm-control

スイッチ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する、またはストーム制御の履歴を表示するには、ユーザ EXEC モードで **show storm-control** コマンドを使用します。

show storm-control [*interface-id*] [**broadcast**| **multicast**| **unicast**]

構文の説明

interface-id	（任意）物理ポートのインターフェイス ID（タイプ、スタック構成可能なスイッチのスタック メンバ、モジュール、ポート番号を含む）。
broadcast	（任意）ブロードキャスト ストームのしきい値設定を表示します。
multicast	（任意）マルチキャスト ストームのしきい値設定を表示します。
unicast	（任意）ユニキャスト ストームのしきい値設定を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

インターフェイスIDを入力しない場合、スイッチ上のすべてのポートに対して1つのトラフィック 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。

次の例では、キーワードを指定せずに入力した **show storm-control** コマンドの出力の一部を示します。トラフィック タイプのキーワードが入力されてないため、ブロードキャスト ストーム制御の設定が表示されます。

```
Device> show storm-control
Interface Filter State  Upper      Lower     Current
--------- ------------- ---------- --------- ---------
Gi1/0/1   Forwarding    20 pps     10 pps    5 pps
Gi1/0/2   Forwarding    50.00%     40.00%    0.00%
<output truncated>
```

次の例では、指定されたインターフェイスの **show storm-control** コマンドの出力を示します。トラフィック タイプのキーワードが入力されてないため、ブロードキャスト ストーム制御の設定が表示されます。

```
Device> show storm-control gigabitethernet 1/0/1
Interface Filter State  Upper      Lower     Current
--------- ------------- ---------- --------- ---------
Gi1/0/1   Forwarding    20 pps     10 pps    5 pps
```

次の表に、show storm-control の出力に表示されるフィールドの説明を示します。

表 *45*：*show storm-control* のフィールドの説明

フィールド	説明
Interface	インターフェイスの ID を表示します。
Filter State	フィルタのステータスを表示します。 • blocking：ストーム制御はイネーブルであり、ストームが発生しています。 • forwarding：ストーム制御はイネーブルであり、ストームは発生していません。 • Inactive：ストーム制御はディセーブルです。
Upper	上限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。

フィールド	説明
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。

関連トピック

storm-control, （1134 ページ）

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 [*map-name*]

構文の説明

map-name	（任意）特定の VLAN アクセス マップ名。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show vlan access-map** コマンドの出力を示します。

```
Device# show vlan access-map
Vlan access-map "vmap4"  10
  Match clauses:
    ip  address: al2
  Action:
    forward
Vlan access-map "vmap4"  20
  Match clauses:
    ip  address: al2
  Action:
    forward
```

関連トピック

show vlan filter, （1132 ページ）

vlan access-map, （1161 ページ）

vlan filter, （1163 ページ）

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*}

構文の説明

access-map *name*	（任意）指定された VLAN アクセス マップのフィルタリング情報を表示します。
vlan *vlan-id*	（任意）指定されたVLANのフィルタリング情報を表示します。指定できる範囲は 1 ～ 4094 です。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、**show vlan filter** コマンドの出力を示します。

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

関連トピック

show vlan access-map, （1131 ページ）

vlan access-map, （1161 ページ）

vlan filter, （1163 ページ）

show vlan group

VLAN グループにマッピングされている VLAN を表示するには、特権 EXEC モードで **show vlan group** コマンドを使用します。

show vlan group [**group-name** *vlan-group-name* **[user_count]**]

構文の説明

group-name *vlan-group-name*	（任意）指定した VLAN グループにマッピングされている VLAN を表示します。
user_count	（任意）特定の VLAN グループにマッピングされている各 VLAN のユーザ数を表示します。

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
Cisco IOS XE 3.2SE	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 group コマンドは既存の VLAN グループを表示し、各 VLAN グループのメンバである VLAN および VLAN の範囲を示します。**group-name** キーワードを入力すると、指定した VLAN グループのメンバのみが表示されます。

次の例では、特定の VLAN グループのメンバを表示する方法を示します。

```
Device# show vlan group group-name group2
vlan group group1 :40-45
```

次に、グループ内の各 VLAN のユーザ数を表示する例を示します。

```
Device# show vlan group group-name group2 user_count
  VLAN     : Count
-------------------
  40         : 5
  41         : 8
  42         : 12
  43         : 2
  44         : 9
  45         : 0
```

関連トピック

vlan group, （1164 ページ）

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て、インターフェイスのしきい値レベルを設定するには、インターフェイス コンフィギュレーション モードで **storm-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。

storm-control {**action** {**shutdown**| **trap**}| {**broadcast**| **multicast**| **unicast**} **level** {*level* [*level-low*]| **bps** *bps* [*bps-low*]| **pps** *pps* [*pps-low*]}}

no storm-control {**action** {**shutdown**| **trap**}| {**broadcast**| **multicast**| **unicast**} **level**}

構文の説明

action	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を指定します。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、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。
shutdown	ストームの間、ポートをディセーブルにします。
trap	ストームが発生した場合に SNMP トラップを送信します。
broadcast	インターフェイス上でブロードキャスト ストーム制御をイネーブルにします。
multicast	インターフェイス上でマルチキャスト ストーム制御をイネーブルにします。

unicast	インターフェイス上でユニキャスト ストーム制御をイネーブルにします。
level	上限および下限抑制レベルをポートの全帯域幅の割合で指定します。
level	上限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。指定した level の値に達した場合、ストーム パケットのフラッディングをブロックします。
level-low	（任意）下限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。この値は上限抑制値より小さいか、または等しくなければなりません。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。
level bps	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（ビット/秒）で指定します。
bps	上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。指定した bps の値に達した場合、ストーム パケットのフラッディングをブロックします。 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。
bps-low	（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は上限抑制値に等しいか、または小さくなければなりません。 大きい数値のしきい値には、k、m、gなどのメトリック サフィクスを使用できます。
level pps	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（パケット/秒）で指定します。
pps	上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。指定した pps の値に達した場合、ストーム パケットのフラッディングをブロックします。 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。
pps-low	（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は上限抑制値に等しいか、または小さくなければなりません。 大きい数値のしきい値には、k、m、gなどのメトリック サフィクスを使用できます。

コマンド デフォルト

ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。

デフォルト アクションは、トラフィックをフィルタリングし、SNMP トラップを送信しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、またはユニキャスト 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）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチは、Open Shortest Path First（OSPF）および通常のマルチキャスト データ トラフィック間のように、ルーティング アップデート間を区別しないため、両方のタイプのトラフィックがブロックされます。

trap および **shutdown** オプションは、互いに独立しています。

パケット ストームが検出されたときにシャットダウンを行う（ストームの間、ポートが error-disabled 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。

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。

```
Device(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。

```
Device(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。

```
Device(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。

```
Device(config-if)# storm-control action shutdown
```

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

関連トピック

show storm-control, （1129 ページ）

switchport port-security aging

セキュア アドレス エントリのエージング タイムおよびタイプを設定する、または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、インターフェイス コンフィギュレーション モードで **switchport port-security aging** コマンドを使用します。ポート セキュリティ エージングをディセーブルにする、またはパラメータをデフォルトの状態に設定するには、このコマンドの **no** 形式を使用します。

switchport port-security aging {**static**| **time** *time*| **type** {**absolute**| **inactivity**}}

no switchport port-security aging {**static**| **time**| **type**}

構文の説明

static	このポートに静的に設定されたセキュア アドレスのエージングをイネーブルにします。

time*time*	このポートのエージング タイムを指定します。指定できる範囲は 0 ～ 1440 分です。time が 0 の場合、このポートのエージングはディセーブルです。
type	エージング タイプを設定します。
absolute	absolute エージング タイプを設定します。このポートのすべてのセキュア アドレスは、指定された時間（分）が経過した後に期限切れとなり、セキュア アドレス リストから削除されます。
inactivity	inactivity エージング タイプを設定します。指定された時間内にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュア アドレスが期限切れになります。

コマンド デフォルト

ポート セキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。

デフォルトのエージング タイプは absolute です。

デフォルトのスタティック エージング動作はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

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。

```
Device(config)# interface gigabitethernet1/0/1
Device(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。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(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。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
```

関連トピック

show interfaces switchport, （212 ページ）

switchport port-security mac-address, （1139 ページ）

switchport port-security maximum, （1142 ページ）

switchport port-security violation, （1144 ページ）

switchport port-security mac-address

セキュア MAC アドレスまたはスティッキ MAC アドレス ラーニングを設定するには、**switchport port-security mac-address** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security mac-address {*mac-address* [**vlan** {*vlan-id* {**access**| **voice**}}]| **sticky** [*mac-address*| **vlan** {*vlan-id* {**access**| **voice**}}]}

no switchport port-security mac-address {*mac-address* [**vlan** {*vlan-id* {**access**| **voice**}}]| **sticky** [*mac-address*| **vlan** {*vlan-id* {**access**| **voice**}}]}

構文の説明

mac-address	48 ビット MAC アドレスの入力によって指定するインターフェイスのセキュア MAC アドレス。設定された最大数まで、セキュア MAC アドレスを追加できます。
vlan*vlan-id*	（任意）トランク ポート上でだけ、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。

vlan access	（任意）アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。
vlan voice	（任意）アクセス ポートでだけ、VLAN を音声 VLAN として指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらに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。
sticky	スティッキ ラーニングのインターフェイスをイネーブルにします。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習したすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。
mac-address	（任意）スティッキ セキュア MAC アドレスを指定する MAC アドレス。

コマンド デフォルト

セキュア MAC アドレスは設定されていません。

スティッキ ラーニングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

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 ポートにすることができますが、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 ポートをギガビットまたは 10 ギガビット 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。

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（スティッキ ラーニングがイネーブルになる前に動的に学習されたアドレスを含む）を、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、これらのアドレスはアドレス テーブルおよび実行コンフィギュレーションに追加されます。ポート セキュリティがディセーブルの場合、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキ セキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくてすみます。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。
- スティッキ ラーニングをディセーブルにして、**switchport port-security mac-address sticky***mac-address* インターフェイス コンフィギュレーション コマンドを入力した場合、エラー メッセージが表示され、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに追加されません。

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。

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。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(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。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

関連トピック

show interfaces switchport, （212 ページ）

switchport port-security aging, （1137 ページ）

switchport port-security maximum, （1142 ページ）

switchport port-security violation, （1144 ページ）

switchport port-security maximum

セキュア MAC アドレス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 **switchport port-security maximum** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security maximum *value* [**vlan** [*vlan-list*| [**access**| **voice**]]]

no switchport port-security maximum *value* [**vlan** [*vlan-list*| [**access**| **voice**]]]

構文の説明

value	インターフェイスのセキュア MAC アドレスの最大数を設定します。 デフォルトの設定は 1 秒です。
vlan	（任意）トランク ポートの場合、VLAN ごとまたは一定範囲の VLAN のセキュア MAC アドレスの最大数を設定します。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。
vlan-list	（任意）カンマで区切られた VLAN の範囲またはハイフンで区切られた一連の VLAN。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。
access	（任意）アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。
voice	（任意）アクセス ポートでだけ、VLAN を音声 VLAN として指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

コマンド デフォルト

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。

コマンド モード

インターフェイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

スイッチまたはスイッチ スタック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。**sdm prefer** コマンドを参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。

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 ポートにすることができます。
- 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 ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。
- 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。

  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。

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。

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。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
```

関連トピック

show interfaces switchport, （212 ページ）

switchport port-security aging, （1137 ページ）

switchport port-security mac-address, （1139 ページ）

switchport port-security violation, （1144 ページ）

switchport port-security violation

セキュア MAC アドレスの違反モード、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 **switchport port-security violation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security violation {**protect**| **restrict**| **shutdown**| **shutdown vlan**}

no switchport port-security violation {**protect**| **restrict**| **shutdown**| **shutdown vlan**}

構文の説明

protect	セキュリティ違反保護モードを設定します。
restrict	セキュリティ違反制限モードを設定します。

shutdown	セキュリティ違反シャットダウン モードを設定します。
shutdown vlan	VLAN ごとのシャットダウンにセキュリティ違反モードを設定します。

コマンド デフォルト

デフォルトの違反モードは、**shutdown** 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

セキュリティ違反保護モードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。ドロップすることでセキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。

（注） トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくてもVLANが保護モードの最大数に達すると、ラーニングがディセーブルになります。

セキュリティ違反制限モードでは、セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。

セキュリティ違反シャットダウンモードでは、違反が発生し、ポートのLEDがオフになると、インターフェイスが errdisable 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 error-disabled 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か、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにすることができます。

セキュリティ違反モードが VLAN ごとのシャットダウンに設定されると、違反が発生した VLAN のみが errdisable になります。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることができます。
- 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 ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。

  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 error-disabled 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 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。

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。

次の例では、MAC セキュリティ違反が発生した場合に VLAN のみをシャットダウンするようポートを設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
```

関連トピック

show interfaces switchport, （212 ページ）

switchport port-security aging, （1137 ページ）

switchport port-security mac-address, （1139 ページ）

switchport port-security maximum, （1142 ページ）

tracking（IPv6 スヌーピング）

ポートでデフォルトのトラッキング ポリシーを上書きするには、IPv6 スヌーピング ポリシー コンフィギュレーション モードで **tracking** コマンドを使用します。

tracking{**enable**[**reachable-lifetime** {*value*| **infinite**}] | **disable**[**stale-lifetime** {*value*| **infinite**}

構文の説明

enable	トラッキングをイネーブルにします。
reachable-lifetime	（任意）到達可能という証明がない状態で、到達可能なエントリが直接的または間接的に到達可能であると判断される最大時間を指定します。 • **reachable-lifetime** キーワードを使用できるのは、**enable** キーワードが指定されている場合のみです。 • **reachable-lifetime** キーワードを使用すると、 **ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムが上書きされます。
value	秒単位のライフタイム値。指定できる範囲は 1 ～ 86400 で、デフォルトは 300 です。
infinite	エントリを無限に到達可能状態またはステイル状態に維持します。
disable	トラッキングをディセーブルにします。
stale-lifetime	（任意）時間エントリをステイル状態に維持します。これによりグローバルの stale-lifetime 設定が上書きされます。 • ステイル ライフタイムは 86,400 秒です。 • **stale-lifetime** キーワードを使用できるのは、**disable** キーワードが指定されている場合のみです。 • **stale-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイル ライフタイムが上書きされます。

コマンド デフォルト

時間のエントリは到達可能な状態に維持されます。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

tracking コマンドは、このポリシーが適用されるポート上で **ipv6 neighbor tracking** コマンドによって設定されたデフォルトのトラッキング ポリシーに優先します。この機能は、たとえば、エントリを追跡しないが、バインディング テーブルにエントリを残して盗難を防止する場合などに、信頼できるポート上で有用です。

reachable-lifetime キーワードは、到達可能という証明がない状態で、あるエントリがトラッキングにより直接的に、またはIPv6スヌーピングにより間接的に到達可能であると判断される最大時間を示します。**reachable-lifetime** 値に到達すると、エントリはステイル状態に移行します。tracking コマンドで **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムが上書きされます。

stale-lifetime キーワードは、エントリが削除されるか、直接または間接的に到達可能であると証明される前にテーブルに保持される最大時間です。**tracking** コマンドで **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイル ライフタイムが上書きされます。

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、エントリを信頼できるポート上で無限にバインディング テーブルに保存するように設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

あるポートを信頼できるポートとして設定するには、IPv6 スヌーピング ポリシー モードまたは ND 検査ポリシー コンフィギュレーション モードで **trusted-port** 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。

trusted-port

no trusted-port

構文の説明

コマンド デフォルト

このコマンドには引数またはキーワードはありません。

NDのポートも信頼されポリシーの設定

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

trusted-port コマンドをイネーブルにすると、メッセージがこのポリシーを持つポートで受信された場合、限定的に実行されるか、まったく実行されません。ただし、アドレス スプーフィングから保護するために、メッセージは伝送するバインディング情報の使用によってバインディング テーブルを維持できるように分析されます。これらのポートで検出されたバインディングは、信頼できるものとして設定されていないポートから受信したバインディングよりも信頼性が高いものと見なされます。

次に、NDP ポリシー名を policy1 と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
Device(config)# ipv6  nd inspection  policy1
Device(config-nd-inspection)# trusted-port
```

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
```

wireless dot11-padding

Over-the-Air フレーム パディングをイネーブルにするには、**wirelessdot11-padding** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

wireless dot11-padding

no wireless dot11-padding

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、Over-the-Air フレーム パディングをイネーブルにする例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless dot11-padding
```

wireless security dot1x

IEEE 802.1x のグローバル コンフィギュレーションを設定するには、**wirelesssecuritydot1x** コマンドを使用します。

wireless security dot1x [**eapol-key** {**retries** *retries*| **timeout** *milliseconds*}| **group-key interval** *sec*| **identity-request** {**retries** *retries*| **timeout** *seconds*}| **radius [call-station-id]** {**ap-macaddress**| **ap-macaddress-ssid**| **ipaddress**| **macaddress**}| **request** {**retries** *retries*| **timeout** *seconds*}| **wep key** {**index 0**| **index 3**}]

構文の説明

eapol-key	eapol-key 関連パラメータを設定します。
retries*retries*	（任意）コントローラが無線クライアントにEAPOL（WPA）キー メッセージを再送信する最大回数（0～4）を指定します。 デフォルト値は 2 です。
timeout*milliseconds*	（任意）EAP または WPA/WPA-2 PSK を使用してコントローラが無線クライアントにEAPOL（WPA）キー メッセージを再送信するまでに待機する時間（200 ～ 5000 ミリ秒）を指定します。 デフォルト値は 1000 ミリ秒です。
group-keyinterval*sec*	EAP ブロードキャスト キーを更新する間隔を秒で設定します（120～86400 秒）。
identity-request	EAP ID 要求の関連パラメータを設定します。

retries*retries*	（任意）コントローラが EAP ID を要求する最大試行回数（0～4）を指定します。 デフォルト値は 2 です。
timeout*seconds*	（任意）コントローラが無線クライアントに EAP ID 要求メッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
radius	RADIUS メッセージを設定します。
call-station-id	（任意）RADIUS メッセージで送信されるコール ステーション ID を設定します。
ap-macaddress	呼出端末 ID タイプを AP の MAC アドレスに設定します。
ap-macaddress-ssid	呼出端末 ID タイプを 'AP の MAC アドレス':'SSID' に設定します。
ipaddress	呼出端末 ID タイプをシステムの IP アドレスに設定します。
macaddress	呼出端末 ID タイプをシステムの MAC アドレスに設定します。
request	EAP 要求の関連パラメータを設定します。
retries*retries*	（任意）ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信する最大回数（0 ～ 20）を指定します。 デフォルト値は 2 です。
timeout*seconds*	（任意）ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
wepkey	802.1x WEP 関連パラメータを設定します。
index0	WEP キーのインデックス値を 0 として指定します。
index3	WEP キーのインデックス値を 3 として指定します。

コマンド デフォルト

eapol-key-timeout のデフォルト値：1 秒。

eapol-key-retries のデフォルト値：2 回。

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

この例では、**wirelesssecuritydot1x** の下のすべてのコマンドを示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

wireless security lsc

ローカルで有効な証明書を設定するには、**wirelesssecuritylsc** コマンドを使用します。

wireless security lsc {**ap-provision** [**auth-list** *mac-addr*| **revert** *number*]| **other-params** *key-size*| **subject-params** *country state city orgn dept email*| **trustpoint** *trustpoint*}

構文の説明

ap-provision	アクセス ポイント プロビジョニング リストの設定を指定します。
auth-list*mac-addr*	プロビジョニング リストの許可設定を指定します。
revert*number*	デフォルトの証明書に戻る前にアクセス ポイントが LSC を使用してコントローラへの接続を試行する回数。最大試行回数は255以下にする必要があります。
other-params*key-size*	デバイスの証明書キーのサイズ設定を指定します。
subject-params*countrystatecityorgndeptemail*	デバイス証明書の設定を指定します。認証局の国、州、市、組織、部門、および電子メール。
trustpoint*trustpoint*	LSC のトラスト ポイントを指定します。

コマンド デフォルト

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

1 つの CA サーバだけを設定できます。別の CA サーバを設定するには、config certificate lsc ca-server delete コマンドを使用して設定済みの CA サーバを削除した後、別の CA サーバを設定します。

アクセス ポイント プロビジョニング リストを設定する場合は、AP プロビジョニングを有効にしたときに（手順 8）プロビジョニング リストのアクセス ポイントだけがプロビジョニングされます。アクセス ポイント プロビジョン リストを設定しない場合、コントローラに接続する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。

次の例に、ローカルで有効な証明書の設定方法を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security lsc ?
  ap-provision    Provisioning the AP's with LSC's
  other-params    Configure Other Parameters for Device Certs
  subject-params  Configure the Subject Parameters for Device Certs
  trustpoint      Configure LSC Trustpoint
  <cr>
```

wireless security strong-password

強力なパスワードの強制オプションを設定するには、**wirelesssecuritystrong-password** コマンドを使用します。強力なパスワ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。

wireless security strong-password

no wireless security strong-password

コマンド デフォルト

なし。

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、ワイヤレス セキュリティのための強力なパスワードを設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security strong-password
```

wireless wps ap-authentication

アクセス ポイントのネイバー認証を設定するには、**wirelesswpsap-authentication** コマンドを使用します。アクセス ポイントのネイバー認証を削除するには、このコマンドの no 形式を使用します。

wireless wps ap-authentication [**threshold** *value*]

no wireless wps ap-authentication [threshold]

構文の説明

threshold*value*	（任意）無線 LAN の WMM 対応クライアントであることを指定します。しきい値（1 ～ 255）。

コマンド デフォルト

なし。

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、WMM 対応クライアントのしきい値を設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps ap-authentication threshold 65
```

wireless wps auto-immune

サービス妨害（DoS）攻撃からの保護をイネーブルにするには、**wirelesswpsauto-immune** コマンドを使用します。ディセーブルにするには、このコマンドの no 形式を使用します。

wireless wps auto-immune

no wireless wps auto-immune

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

潜在的な攻撃者は特別に作成したパケットを使用し、正規のクライアントを攻撃者として処理するように侵入検知システム（IDS）を誘導する場合があります。それによって、コントローラはこの正規のクライアントの接続を解除し、DoS 攻撃が開始されます。自己免疫機能は、有効な場合にこのような攻撃を防ぐように設計されています。ただし、自己免疫機能を有効にすると、Cisco 792x フォンを使用した会話が断続的に中断されることがあります。792x フォンを使用しているときに頻繁に中断されるようであれば、この機能を無効にしてください。

次の例では、サービス妨害（DoS）攻撃からの保護をイネーブルにする方法を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps auto-immune
```

wireless wps cids-sensor

Wireless Protection System（WPS）の侵入検知システム（IDS）センサーを設定するには、**wirelesswpscids-sensor** コマンドを使用します。Wireless Protection System（WPS）の侵入検知システム（IDS）セン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。

wireless wps cids-sensor *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*]

no wireless wps cids-sensor *index*

構文の説明

index	IDS センサーの内部インデックスを指定します。
ip-address*ip-addr***username***username***password***password_type**password*	IDS センサーの IP アドレス、IDS センサーのユーザ名、パスワード タイプ、および IDS センサーのパスワードを指定します。

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし

次に、IDS インデックス、IDS センサーの IP アドレス、IDS ユーザ名およびパスワードを使用して侵入検知システムを設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps cids-sensor 1 10.0.0.51 Sensor_user0doc1 passowrd01
```

wireless wps client-exclusion

クライアント除外ポリシーを設定するには、**wireless wps client-exclusion** コマンドを使用します。クライアント除外ポリシーを削除するには、このコマンドの **no** 形式を使用します。

wireless wps client-exclusion {**all**| **dot11-assoc**| **dot11-auth**| **dot1x-auth**| **ip-theft**| **web-auth**}

no wireless wps client-exclusion {**all**| **dot11-assoc**| **dot11-auth**| **dot1x-auth**| **ip-theft**| **web-auth**}

構文の説明

dot11-assoc	コントローラが 802.11 アソシエーションに連続 5 回失敗すると、6 回目の試行を除外することを指定します。
dot11-auth	コントローラが 802.11 認証に連続 5 回失敗すると、6 回目の試行を除外することを指定します。
dot1x-auth	コントローラが 802.11X 認証に連続 5 回失敗すると、6 回目の試行を除外することを指定します。
ip-theft	IP アドレスがすでに別のデバイスに割り当てられている場合は、コントローラがクライアントを除外することを指定します。 詳細については、「使用上のガイドライン」セクションを参照してください。
web-auth	コントローラが Web 認証に連続 3 回失敗すると、4 回目の試行を除外することを指定します。
all	コントローラが上記のすべての理由でクライアントを除外することを指定します。

コマンド デフォルト

イネーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 窃盗シナリオに、古い Cisco IOS XE リリースと Cisco IOS XE Denali 16.x リリースの相違点があります。

古い Cisco IOS XE リリース	Cisco IOS XE Denali 16.x リリース
優先順位に従って、有線クライアントはワイヤレスクライアントよりも優先され、DHCP IP はスタティック IP よりも優先されます。クライアントのセキュリティタイプはチェックされません。すべてのクライアントタイプのセキュリティが同じ優先順位で処理されます。 既存のバインドが優先順位の高いソースに由来する場合、新しいバインドは無視され、IP 窃盗の信号が送信されます。既存のバインドが新しいバインドと同じ優先順位のソースに由来する場合、新しいバインドは無視され、IP 窃盗の信号が送信されます。その結果、2 つのホストが同じ IP を使用してトラフィックを送信した場合、バインドは切り替わらないことになります。最初のバインドのみがソフトウェアに格納されます。新しいバインドが優先順位のより高いソースに由来する場合、既存のバインドは置き換えられます。その結果、既存のバインドの IP 窃盗通知と、新しいバインドの通知が送信されます。	有線とワイヤレスの間に基本的な相違はありません。重視されるのは、エントリの信頼性（優先度）、エントリの伝達経路となった機能（ARP、DHCP、ND など）、およびポートに付与されているポリシーです。優先度が等しい場合、古いエントリが到達可能であれば、IP テイクオーバーは拒否されます。IP テイクオーバーは、更新が信頼できるポートから発信され、新しいエントリが DHCP サーバから IP アドレスを取得した場合に発生します。そうでない場合には、明示的に許可する必要があります。古いエントリが新しいより信頼できるエントリに置き換えられた場合、IP 窃盗は報告されません。

次に、802.11 アソシエーションに連続 5 回失敗した場合にクライアントを無効にする例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp infrastructure

管理フレーム保護（MFP）を設定するには、**wirelesswpsmfpinfrastructure** コマンドを使用します。管理フレーム保護（MFP）を削除するには、このコマンドの no 形式を使用します。

wireless wps mfp infrastructure

no wireless wps mfp infrastructure

コマンド デフォルト

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、インフラストラクチャ MFP を有効にする例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps mfp infrastructure
```

wireless wps rogue

さまざまな不正パラメータを設定するには、**wirelesswpsrogue** コマンドを使用します。

wireless wps rogue {**adhoc**| **client**} [**alert** *mac-addr*| **contain** *mac-addr no-of-aps*]

構文の説明

adhoc	Independent Basic Service Set（IBSS またはアドホック）の不正なアクセス ポイントのステータスを設定します。
client	不正なクライアントを設定します。
alert*mac-addr*	アドホックの不正を検出すると SNMP トラップを生成し、システム管理者に即座にアラートを発信して、アドホックの不正アクセス ポイントの MAC アドレスに対し必要な措置を促します。
contain*mac-addrno-of-aps*	加害デバイスを阻止し、その信号が正規クライアントを阻害しないようにします。 アドホックの不正なアクセス ポイントをアクティブに阻止するために割り当てられた、シスコのアクセス ポイントの最大数（1 ～ 4）。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、システム管理者に即座にアラートを生成し、アドホックの不正アクセス ポイントの MAC アドレスに対し必要な措置を促す例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps rouge adhoc alert mac_addr
```

wireless wps shun-list re-sync

回避リストのコントローラをモビリティ グループ内の他のコントローラと同期させるには、**wirelesswpsshun-listre-sync** コマンドを使用します。

wireless wps shun-list re-sync

コマンド デフォルト

なし。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、回避リストのコントローラを他のコントローラと同期するように設定する例を示します。

```
Device#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps shun-list re-sync
```

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し、VLAN アクセス マップ コンフィギュレーション モードに変更するには、スイッチ スタックまたはスタンドアロン スイッチのグローバル コンフィギュレーション モードで **vlan access-map** コマンドを使用します。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 access-map *name* [*number*]

no vlan access-map *name* [*number*]

（注） このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

構文の説明

name	VLAN マップ名
number	（任意）作成または変更するマップ エントリのシーケンス番号（0 ～ 65535）。VLAN マップを作成する際にシーケンス番号を指定しない場合、番号は自動的に割り当てられ、10 から開始して 10 ずつ増加します。この番号は、VLAN アクセス マップ エントリに挿入するか、または VLAN アクセス マップ エントリから削除する順番です。

コマンド デフォルト

VLAN に適用する VLAN マップ エントリまたは VLAN マップはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

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、照合する IP または非 IP トラフィックのアクセス リストを指定できます。また、**action** コマンドを使用して、この照合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（forward または drop）。
- **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、デフォルト値に設定します。

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、エントリを個別に削除できます。

VLAN マップを 1 つまたは複数の VLAN に適用するには、**vlan filter** インターフェイス コンフィギュレーション コマンドを使用します。

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。

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。

```
Device(config)# vlan access-map vac1
Device(config-access-map)# match ip address acl1
Device(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。

```
Device(config)# no vlan access-map vac1
```

関連トピック

action, （1027 ページ）

match（アクセス マップ コンフィギュレーション）, （1092 ページ）

show vlan access-map, （1131 ページ）

vlan filter, （1163 ページ）

vlan filter

1 つ以上の VLAN に VLAN マップを適用するには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **vlan filter** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

vlan filter *mapname* **vlan-list** {*list*| **all**}

no vlan filter *mapname* **vlan-list** {*list*| **all**}

（注） このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

構文の説明

mapname	VLAN マップ エントリ名
vlan-list	マップを適用する VLAN を指定します。
list	tt、uu-vv、xx、および yy-zz 形式での 1 つまたは複数の VLAN リスト。カンマとダッシュの前後のスペースは任意です。指定できる範囲は 1 ～ 4094 です。
all	マップをすべての VLAN に追加します。

コマンド デフォルト

VLAN フィルタはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

パケットを誤って過剰にドロップし、設定プロセスの途中で接続が無効になることがないように、VLAN アクセス マップを完全に定義してから VLAN に適用することを推奨します。

VLAN マップ エントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

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。

```
Device(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。

```
Device(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。

関連トピック

show vlan access-map, （1131 ページ）

show vlan filter, （1132 ページ）

vlan access-map, （1161 ページ）

vlan group

VLAN グルー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 **vlan group** コマンドを使用します。VLAN グループから VLAN 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。

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

構文の説明

group-name	VLAN グループの名前。名前は最大 32 文字で、文字から始める必要があります。
vlan-list *vlan-list*	VLAN グループに追加される 1 つ以上の VLAN を指定します。*vlan-list* 引数には単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲を指定できます。複数のエントリはハイフン（-）またはカンマ（,）で区切ります。

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
Cisco IOS XE 3.2SE	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 VLAN グループが存在しない場合、**vlan group** コマンドはグループを作成し、指定された VLAN リストをそのグループにマッピングします。指定された VLAN グループが存在する場合は、指定された VLAN リストがそのグループにマッピングされます。

vlan group コマンドの **no** 形式を使用すると、指定された VLAN リストが VLAN グループから削除されます。VLAN グループから最後の VLAN を削除すると、その VLAN グループは削除されます。

最大 100 の VLAN グループを設定でき、1 つの VLAN グループに最大 4094 の VLAN をマッピングできます。

次に、VLAN 7 ～ 9 と 11 を VLAN グループにマッピングする例を示します。

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

次の例では、VLAN グループから VLAN 7 を削除する方法を示します。

```
Device(config)# no vlan group group1 vlan-list 7
```

関連トピック

show vlan group, （1133 ページ）

第 XVIII 部

スタック マネージャおよびハイ アベイラビリティ

- スタック マネージャおよびハイ アベイラビリティ コマンド，1169 ページ
- StackWise Virtual コマンド，1221 ページ

第 19 章

スタック マネージャおよびハイ アベイラビリティ コマンド

- debug platform stack-manager, 1170 ページ
- main-cpu, 1171 ページ
- mode sso, 1172 ページ
- policy config-sync prc reload, 1173 ページ
- redundancy, 1174 ページ
- redundancy config-sync mismatched-commands, 1175 ページ
- redundancy force-switchover, 1177 ページ
- redundancy reload, 1178 ページ
- reload, 1179 ページ
- session, 1180 ページ
- set trace capwap ap ha, 1181 ページ
- set trace mobility ha, 1183 ページ
- set trace qos ap ha, 1185 ページ
- show checkpoint, 1186 ページ
- show etherchannel summary, 1191 ページ
- show platform ses, 1192 ページ
- show platform stack-manager, 1197 ページ
- show redundancy, 1198 ページ
- show redundancy config-sync, 1202 ページ
- show switch, 1204 ページ

- show trace messages capwap ap ha, 1209 ページ
- show trace messages mobility ha, 1210 ページ
- stack-mac persistent timer, 1211 ページ
- stack-mac update force, 1212 ページ
- standby console enable, 1213 ページ
- switch stack port, 1214 ページ
- switch priority, 1216 ページ
- switch provision, 1217 ページ
- switch renumber, 1219 ページ

debug platform stack-manager

スタック マネージャ ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform stack-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には、このコマンドの **no** 形式を使用します。

debug platform stack-manager {**level1**| **level2**| **level3**| **sdp**| **serviceability**| **sim**| **ssm**| **trace**} [**switch** *switch-number*]

no debug platform stack-manager {**level1**| **level2**| **level3**| **sdp**| **serviceability**| **sim**| **ssm**| **trace**} [**switch** *switch-number*]

構文の説明

level1	レベル 1 のデバッグ ログをイネーブルにします。
level2	レベル 2 のデバッグ ログをイネーブルにします。
level3	レベル 3 のデバッグ ログをイネーブルにします。
sdp	スタック ディスカバリ プロトコル（SDP）のデバッグ メッセージを表示します。
サービスアビリティ	スタック マネージャ サービスアビリティのデバッグ メッセージを表示します。
sim	スタック情報モジュールのデバッグ メッセージを表示します。
ssm	スタック ステートマシンのデバッグ メッセージを表示します。
trace	スタック マネージャの入口と出口のデバッグ メッセージを追跡します。

switch *switch-number*	（任意）デバッグ オンをイネーブルにするスタック メンバー番号を指定します。指定できる範囲は 1 ～ 9 です。

コマンド 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
Cisco IOS XE 3.2SE	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、スタック対応スイッチのみでサポートされています。

undebug platform stack-manager コマンドは、**no debug platform stack-manager** コマンドと同じです。

main-cpu

冗長メイン コンフィギュレーション サブモードを開始し、スタンバイ スイッチを有効にするには、冗長コンフィギュレーション モードで **main-cpu** コマンドを使用します。

main-cpu

構文の説明

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

冗長コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

冗長メイン コンフィギュレーション サブモードから、**standby console enable** コマンドを使用してスタンバイ スイッチを有効にします。

次に、冗長メイン コンフィギュレーション サブモードを開始し、スタンバイ スイッチをイネーブルにする例を示します。

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device#
```

関連トピック

standby console enable, （1213 ページ）

mode sso

冗長モードをステートフル スイッチオーバー（SSO）に設定するには、冗長コンフィギュレーション モードで **mode sso** コマンドを使用します。

mode sso

構文の説明

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

冗長コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

mode sso コマンドは、冗長コンフィギュレーション モードでのみ入力できます。

システムを SSO モードに設定する場合は、次の注意事項に従ってください。

- SSO モードをサポートするために、スタック内のスイッチでは同一の Cisco IOS イメージを使用する必要があります。Cisco IOS リリース間の相違のために、冗長機能が動作しない場合があります。
- モジュールの活性挿抜（OIR）を実行する場合、モジュールの状態が移行状態（Ready 以外の状態）である場合にだけ、ステートフル スイッチオーバーの間にスイッチはリセットし、ポート ステートは再起動します。
- 転送情報ベース（FIB）テーブルはスイッチオーバー時に消去されます。ルーテッド トラフィックは、ルート テーブルが再コンバージェンスするまで中断されます。

次の例では、冗長モードを SSO に設定する方法を示します。

```
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)#
```

policy config-sync prc reload

Parser Return Code（PRC）の障害がコンフィギュレーションの同期中に発生した場合にスタンバイ スイッチをリロードするには、冗長コンフィギュレーション モードで **policy config-sync reload** コマンドを使用します。Parser Return Code（PRC）の障害が発生した場合にスタンバイ スイッチがリロードしないように指定するには、このコマンドの **no** 形式を使用します。

policy config-sync {**bulk**| **lbl**}**prc reload**

no policy config-sync {**bulk**| **lbl**}**prc reload**

構文の説明

bulk	バルク コンフィギュレーション モードを指定します。
lbl	1 行ごと（lbl）のコンフィギュレーション モードを指定します。

コマンド デフォルト

このコマンドは、デフォルトではイネーブルです。

コマンド モード

冗長コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、Parser Return Code（PRC）の障害がコンフィギュレーションの同期化中に発生した場合に、スタンバイ スイッチがリロードされないように指定する例を示します。

```
Device(config-red)# no policy config-sync bulk prc reload
```

redundancy

冗長コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **redundancy** コマンドを使用します。

redundancy

構文の説明

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

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

冗長コンフィギュレーションモードは、スタンバイ スイッチをイネーブルにするために使用されるメイン CPU サブモードを開始するために使用されます。

メイン CPU サブモードを開始するには、冗長コンフィギュレーション モードで **main-cpu** コマンドを使用します。

スタンバイ スイッチを有効にするには、メイン CPU サブモードから **standby console enable** コマンドを使用します。

冗長コンフィギュレーション モードを終了するには、**exit** コマンドを使用します。

次に、冗長コンフィギュレーション モードを開始する例を示します。

```
Device(config)# redundancy
Device(config-red)#
```

次の例では、メイン CPU サブモードを開始する方法を示します。

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)#
```

redundancy config-sync mismatched-commands

アクティブ スイッチとスタンバイ スイッチの間に設定の不一致があるときにスタンバイ スイッチのスタックへの参加を許可するには、特権 EXEC モードで **redundancy config-sync mismatched-commands** コマンドを使用します。

redundancy config-sync {**ignore**| **validate**} **mismatched-commands**

構文の説明

ignore	Mismatched Command List を無視します。
validate	修正した実行コンフィギュレーションに基づいて Mismatched Command List を再確認します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

スタンバイ スイッチの起動中にアクティブ スイッチの実行コンフィギュレーションのコマンド構文チェックが失敗した場合、**redundancy config-sync mismatched-commands** コマンドを使用して、アクティブ スイッチの Mismatched Command List（MCL）を表示し、スタンバイ スイッチをリブートします。

次に、不一致コマンドのログ エントリの例を示します。

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
! <submode> "interface"
- ip address 192.0.2.0 255.255.255.0
! </submode> "interface"
```

すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブ スイッチの実行コンフィギュレーションからすべての不一致コマンドを除外します。
2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイ スイッチをリロードします。

次の手順に従って、MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイ スイッチをリロードします。システムは SSO モードに移行します。

（注） 不一致コマンドを無視する場合、アクティブ スイッチとスタンバイ スイッチの同期していないコンフィギュレーションは存在したままです。

3. 無視した MCL を **show redundancy config-sync ignored mcl** コマンドで確認します。

コンフィギュレーション ファイルの互換性の問題が原因で、アクティブ スイッチとスタンバイ スイッチ間で SSO モードを確立できない場合、Mismatched Command List（MCL）がアクティブ スイッチで生成され、スタンバイ スイッチに対して Route Processor Redundancy（RPR）モードへのリロードが強制されます。

（注） RPR モードはエラーの場合にフォール バックとして Catalyst 3850 スイッチでサポートされています。これは設定可能ではありません。

障害となっているコンフィギュレーションを削除し、スタンバイ スイッチを同じイメージで再起動した後に SSO の確立を試行する場合、ピア イメージが非互換としてリストされているため、C3K_REDUNDANCY-2-IOS_VERSION_CHECK_FAIL および ISSU-3-PEER_IMAGE_INCOMPATIBLE メッセージが表示されます。ピアが STANDBY COLD（RPR）状態のときに、**redundancy config-sync ignore mismatched-commands** EXEC コマンドで、非互換リストからピア イメージをクリアできます。このアクションによって、スタンバイ スイッチを、リロード時に STANDBY HOT（SSO）ステートで起動できます。

次の例に、変更したコンフィギュレーションとの Mismatched Command List を再検証する方法を示します。

```
Device# redundancy config-sync validate mismatched-commands
Device#
```

redundancy force-switchover

アクティブ スイッチとスタンバイ スイッチのスイッチオーバーを強制的に実行するには、スイッチ スタックの特権 EXEC モードで **redundancy force-switchover** コマンドを使用します。

redundancy force-switchover

構文の説明

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

手動で冗長スイッチに切り替えるには、**redundancy force-switchover** コマンドを使用します。冗長スイッチは Cisco IOS イメージを実行する新しいアクティブ スイッチになり、モジュールはデフォルト設定にリセットされます。

古いアクティブ スイッチは新しいイメージで再起動し、スタックに参加します。

アクティブ スイッチで **redundancy force-switchover** コマンドを使用すると、アクティブ スイッチのスイッチ ポートがダウン状態になります。

部分リング スタック内のスイッチにこのコマンドを使用すると、次の警告メッセージが表示されます。

```
Device# redundancy force-switchover
Stack is in Half ring setup; Reloading a switch might cause stack split
This will reload the active unit and force switchover to standby[confirm]
```

次の例では、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンに手動で切り替える方法を示します。

```
Device# redundancy force-switchover
Device#
```

redundancy reload

スタック内のいずれか、またはすべてのスイッチを強制リロードするには、特権 EXEC モードで **redundancy reload** コマンドを使用します。

redundancy reload {**peer**| **shelf**}

構文の説明

peer	ピア ユニットをリロードします。
shelf	スタック内のすべてのスイッチが再起動します。

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
Cisco IOS XE 3.2SE	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前に、詳細情報について*Stacking Configuration Guide*（*Catalyst 3850 Switches*）の「Performing a Software Upgrade」の項を参照してください。

スタック内のすべてのスイッチをリブートするには、**redundancy reload shelf** コマンドを使用します。

次に、手動でスタック内のすべてのスイッチをリロードする例を示します。

```
Device# redundancy reload shelf
Device#
```

reload

スタック メンバをリロードし、設定変更を適用するには、特権 EXEC モードで **reload** コマンドを使用します。

reload [**/noverify**| **/verify**] [*LINE*| **at**| **cancel**| **in**| **slot** *stack-member-number*| **standby-cpu**]

構文の説明

/noverify	（任意）リロードの前にファイル シグニチャを確認しないように指定します。
/verify	（任意）リロードの前にファイル シグニチャを確認します。
LINE	（任意）リセットの理由。
at	（任意）リロードを実行する時間を hh:mm 形式で指定します。
cancel	（任意）保留中のリロードをキャンセルします。
in	（任意）リロードを実行する間隔を指定します。
slot	（任意）指定したスタック メンバーに変更を保存し、再起動します。
stack-member-number	（任意）変更を保存するスタック メンバ番号。指定できる範囲は 1 ～ 9 です。
standby-cpu	（任意）スタンバイ ルート プロセッサ（RP）をリロードします。

コマンド デフォルト

スタック メンバをただちにリロードし、設定の変更を有効にします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 スタックに複数のスイッチがある場合に **reload slot***stack-member-number* コマンドを入力すると、設定の保存を要求するプロンプトが表示されません。

次の例では、スイッチ スタックをリロードする方法を示します。

```
Device# reload
System configuration has been modified. Save? [yes/no]: yes
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm] yes
```

次の例では、特定のスタック メンバをリロードする方法を示します。

```
Device# reload slot 6
Proceed with reload? [confirm] y
```

次の例では、単一スイッチのスイッチ スタック（メンバ スイッチが 1 つだけ）をリロードする方法を示します。

```
Device# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

関連トピック

show switch, （1204 ページ）

switch priority, （1216 ページ）

switch renumber, （1219 ページ）

session

特定のスタック メンバの診断シェルまたはスタンバイ Deviceの Cisco IOS プロンプトにアクセスするには、アクティブ Device上の特権 EXEC モードで **session** コマンドを使用します。

session {**standby ios**| **switch** [*stack-member-number*]}

構文の説明

standby ios	スタンバイDeviceの Cisco IOS プロンプトにアクセスします。 （注） このコマンドを使用してスタンバイDeviceを設定することはできません。
switch	スタック メンバの診断シェルにアクセスします。

stack-member-number	（任意）アクティブ スイッチ からアクセスするスタック メンバの番号。範囲は 1 ～ 9 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

スタンバイDeviceでCisco IOSプロンプトにアクセスした場合、システム プロンプトに `-stby` が付加されます。スタンバイDeviceを `Device-stby>` プロンプトで設定することはできません。

スタック メンバの診断シェルにアクセスした場合、システム プロンプトに `(diag)` が付加されます。

次の例では、スタック メンバ 3 にアクセスする方法を示します。

```
Device# session switch 3
Device(diag)>
```

次の例では、スタンバイDeviceにアクセスする方法を示します。

```
Device# session standby ios
Device-stby>
```

関連トピック

reload, （1179 ページ）

show switch, （1204 ページ）

switch priority, （1216 ページ）

switch renumber, （1219 ページ）

set trace capwap ap ha

ワイヤレス アクセス ポイントの制御およびプロビジョニングのハイ アベイラビリティを追跡するには、**set trace capwap ap ha** 特権 EXEC コマンドを使用します。

set trace capwap ap ha [**detail**| **event**| **dump** | {**filter** [**none** [**switch** *switch*]| *filter_name* [*filter_value* [**switch** *switch*]]]| **filtered***switch***level** {**default**| *trace_level*} [**switch** *switch*]}]

構文の説明

detail	（任意）ワイヤレス CAPWAP HA の詳細を指定します。
event	（任意）ワイヤレス CAPWAP HA イベントを指定します。
dump	（任意）ワイヤレス CAPWAP HA の出力を指定します。
filter*mac*	MAC アドレスを指定します。
switch switch number	スイッチ番号を指定します。
none	（任意）フィルタ オプションを指定しません。
switch*switch*	（任意）デバイス番号を指定します。
filter name	適用されたフラグ フィルタ名を追跡します。
filter_value	（任意）フィルタの値。
switch*switch*	（任意）デバイス番号を指定します。
filtered	フィルタ処理されたトレース メッセージを指定します。
switch	スイッチ番号を指定します。
level	トレース レベルを指定します。
default	解除されたトレース レベル値を指定します。
trace_level	トレース レベルを指定します。
switch*switch*	（任意）デバイス番号を指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ワイヤレス CAPWAP HA を表示する例を示します。

```
Device# set trace capwap ap ha detail filter mac WORD switch number
```

set trace mobility ha

スイッチでワイヤレス モビリティ ハイ アベイラビリティをデバッグするには、**set trace mobility ha** 特権 EXEC コマンドを使用します。

set trace mobility ha [**event**| **detail**| **dump**] {**filter**[**mac** *WORD switch switch number*] [**none** [**switch** *switch*]| *filter_name* [*filter_value* [**switch** *switch*]]]| **level** {**default**| *trace_level*} [**switch** *switch*]{**filtered**| *switch*}}

構文の説明

event	（任意）ワイヤレスモビリティ ハイアベイラビリティのイベントを指定します。
detail	（任意）ワイヤレスモビリティ ハイアベイラビリティの詳細を指定します。
dump	（任意）ワイヤレスモビリティ ハイアベイラビリティの出力を指定します。
filter	トレース適用フラグフィルタを指定します。
mac	MAC アドレスを指定します。
WORD switch	スイッチを指定します。
switch number	スイッチ番号を指定します。値の範囲は 1 ～ 4 です。
none	トレース適用フラグフィルタを指定しません。

switch*switch*	（任意）デバイス番号を指定します。
filter_name	適用されたフラグ フィルタ名を追跡します。
filter_value	適用されたフラグ フィルタの値を追跡します。
switch*switch*	デバイス番号を指定します。
level	トレース レベル値を指定します。
default	解除されたトレース レベル値を指定します。
trace_level	トレース レベル値を指定します。
switch*switch*	デバイス番号を指定します。
filtered	フィルタ処理されたトレース メッセージを指定します。
switch	スイッチを指定します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ワイヤレス モビリティ ハイ アベイラビリティの詳細を表示する例を示します。

```
Device# set trace mobility ha detail filter mac WORD
[08/27/13 10:38:35.349 UTC 1 8135] Invalid src ip: 169.254.1.1
```

```
[08/27/13 10:38:35.349 UTC 2 8135] Invalid sysIp: Skip plumbing MC-MA
tunnels.
[08/27/13 10:38:54.393 UTC 3 8135] Mobility version mismatch, v10 received,
 or m
sglen mismatch msglen=74 recvBytes=0, dropping
```

set trace qos ap ha

ワイヤレス サービス品質（QoS）ハイ アベイラビリティをトレースするには、**set trace qos ap ha** 特権 EXEC コマンドを使用します。

set trace QOS ap ha[**event**| **error**] {**filter** [**MACnone** [**switch** *switch*]| *filter_name* [*filter_value* [**switch** *switch*]]]| **level** {**default**| *trace_level*} [**switch** *switch*]}

構文の説明

event	（任意）トレース QoS ワイヤレス AP イベントを指定します。
event *mac*	AP の MAC アドレスを指定します。
event *none*	MAC アドレス値を指定しません。
error	（任意）トレース QoS ワイヤレス AP エラーを指定します。
error *mac*	AP の MAC アドレスを指定します。
error *none*	値を指定しません。
filter	トレース適用フラグ フィルタを指定します。
filter *mac*	AP の MAC アドレスを指定します。
filter *none*	値を指定しません。
switch*switch*	スイッチ番号を指定します。
filter_name	（任意）スイッチ フィルタの名前を指定します。
filter_value	（任意）スイッチ フィルタの値を指定します。値は 1 です。
switch*switch*	（任意）スイッチ番号を指定します。値は 1 です。
level	トレース レベルを指定します。
default	トレース QoS ワイヤレス AP デフォルトを指定します。
trace_level	トレース レベルです。
switch*switch*	（任意）スイッチ番号を指定します。値は 1 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ワイヤレス QoS ハイ アベイラビリティを追跡する例を示します。

```
Device# set trace QOS ap ha
```

show checkpoint

チェックポイント ファシリティ（CF）のサブシステムに関する情報を表示するには、**show checkpoint** コマンドを使用します。

show checkpoint clients entities statistics

構文の説明

clients	チェックポイント クライアントに関する詳細情報を表示します。
entities	チェックポイント エンティティに関する詳細情報を表示します。
statistics	チェックポイント統計情報に関する詳細情報を表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、すべての CF クライアントを表示する例を示します。

```
   Client residing in process  : 8135
------------------------------------------------------------------------------
```

```
Checkpoint client: WCM_MOBILITY
    Client ID                   : 24105
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 6
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_DOT1X
    Client ID                   : 24106
    Total DB inserts            : 2
    Total DB updates            : 1312
    Total DB deletes            : 2
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_APFROGUE
    Client ID                   : 24107
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_CIDS
    Client ID                   : 24110
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_NETFLOW
    Client ID                   : 24111
    Total DB inserts            : 7
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_MCAST
    Client ID                   : 24112
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: wcm_comet
    Client ID                   : 24150
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
--------------------------------------------------------------------------------

All iosd checkpoint clients

--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                          ID         ID       Mode
--------------------------------------------------------------------------------
Network RF Client           3         --       Off

  Total API Messages Sent:                      0
```

```
  Total Transport Messages Sent:                0
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
SNMP CF Client             12         --       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                0
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Online Diags HA            14         --       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                0
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
```

```
                           ID         ID       Mode
------------------------------------------------------------------------------
ARP                        22         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Tableid CF                 27         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Event Manager              33          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
```

```
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
LAN-Switch Port Mana       35          0       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:               --
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
LAN-Switch PAgP/LACP       36          0       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:               --
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
LAN-Switch VLANs           39          0       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:               --
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
```

```
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
```

次に、すべての CF エンティティを表示する例を示します。

```
KATANA_DOC#show checkpoint entities
                        Check Point List of Entities

 CHKPT on ACTIVE server.

------------------------------------------------------------------------------
Entity ID         Entity Name
------------------------------------------------------------------------------
        0         CHKPT_DEFAULT_ENTITY

  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Total Number of Members:            10

  Member(s) of entity 0 are:
    Client ID          Client Name
-----------------------------------------
          168          DHCP Snooping
          167          IGMP Snooping
           41          Spanning-tree
           40          AUTH MGR CHKPT CLIEN
           39          LAN-Switch VLANs
           33          Event Manager
           35          LAN-Switch Port Mana
           36          LAN-Switch PAgP/LACP
          158          Inline Power Checkpoint
```

次に、CF の統計情報を表示する例を示します。

```
KATANA_DOC#show checkpoint statistics
        IOSd Check Point Status
 CHKPT on ACTIVE server.

Number Of Msgs In Hold Q:              0
CHKPT MAX Message Size:                0
TP MAX Message Size:               65503
CHKPT Pending Msg Timer:             100 ms

  FLOW_ON  total:                      0
  FLOW_OFF total:                      0
  Current FLOW status is:             ON
  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Rcv  Msg Q Peak:                     0
  Hold Msg Q Peak:                     0
  Buffers Held Peak:                   0
  Current Buffers Held:                0
  Huge Buffers Requested:              0
```

show etherchannel summary

コントローラのポート、ポートチャネルおよびプロトコルの詳細を表示するには、**show etherchannel summary** コマンドを使用します。

show ethernet summary

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

特権モード。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、コントローラのポート、ポート チャネルおよびプロトコルの詳細を表示する例を示します。

```
controller#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SD)          -
23     Po23(SD)         -
```

show platform ses

プラットフォーム情報（コントローラのスタック イベント シーケンサ）を表示するには、特権 EXEC モードで **show platform ses** を使用します。

show platform ses clients states

構文の説明

clients	SES クライアント リストを表示します。
states	SES カードの状態を表示します。

コマンド デフォルト

なし。

コマンド モード

特権 EXEC モード。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

SES クライアントおよび状態の詳細を表示するには、特権 EXEC モードでこのコマンドを使用します。

次に、スタック イベント シーケンサの状態を表示する例を示します。

```
Card #  Card State
======  ==========
1       NG3K_SES_CARD_ADD_COMPLETED(51)
2       NG3K_SES_CARD_EMPTY(0)
3       NG3K_SES_CARD_EMPTY(0)
4       NG3K_SES_CARD_EMPTY(0)
5       NG3K_SES_CARD_EMPTY(0)
6       NG3K_SES_CARD_EMPTY(0)
7       NG3K_SES_CARD_EMPTY(0)
8       NG3K_SES_CARD_EMPTY(0)
9       NG3K_SES_CARD_EMPTY(0)
```

次に、スタック イベント シーケンサのすべての関連クライアントを表示する例を示します。

```
clientID  = 5
clientSeq = 5
clientName = "MATM"
clientCallback @ 0xF49F7300
next = 0x909194B4

clientID  = 6
clientSeq = 6
clientName = "L2 CONTROL"
clientCallback @ 0xF49CA3F0
next = 0x915E4E80

clientID  = 7
clientSeq = 7
clientName = "CDP"
clientCallback @ 0xF49C7220
next = 0x915E4F08

clientID  = 8
clientSeq = 8
clientName = "UDLD"
clientCallback @ 0xF49C75D0
next = 0x91854CA0
```

```
clientID  = 9
clientSeq = 9
clientName = "LLDP"
clientCallback @ 0xF49E62F0
next = 0x90919F90

clientID  = 10
clientSeq = 10
clientName = "L2M"
clientCallback @ 0xF49CE4D0
next = 0x90E35A5C

clientID  = 11
clientSeq = 11
clientName = "Storm-Control"
clientCallback @ 0xF4BA8080
next = 0x9089E9B4

clientID  = 12
clientSeq = 12
clientName = "Security Utils"
clientCallback @ 0xF466BFB0
next = 0x91855F14

clientID  = 13
clientSeq = 13
clientName = "BACKUP-INT"
clientCallback @ 0xF4A191B0
next = 0x91D3511C

clientID  = 14
clientSeq = 14
clientName = "SPAN"
clientCallback @ 0xF4A34F30
next = 0x90FFC8C8

clientID  = 15
clientSeq = 15
clientName = "NG3K_SES_CLIENT_SECURITY_CTRL"
clientCallback @ 0xF4CD1D80
next = 0x95AE5834

clientID  = 16
clientSeq = 16
clientName = "NG3K_SES_CLIENT_DAI"
clientCallback @ 0xF4CD0C50
next = 0x95AE4854

clientID  = 17
clientSeq = 17
clientName = "NG3K_SES_CLIENT_DHCPSN"
clientCallback @ 0xF4CA9D30
next = 0x91DF7728

clientID  = 18
clientSeq = 18
clientName = "NG3K_SES_CLIENT_IPSG"
clientCallback @ 0xF4CDED70
next = 0x9131DCD8

clientID  = 20
clientSeq = 20
clientName = "DTLS"
clientCallback @ 0xF49B2CB0
next = 0x9134508C

clientID  = 21
clientSeq = 21
clientName = "STATS"
clientCallback @ 0xF49BD750
next = 0x9134746C

clientID  = 22
```

```
clientSeq = 22
clientName = "PLATFORM_MGR"
clientCallback @ 0xF4AB2D40
next = 0x91323D20

clientID  = 23
clientSeq = 23
clientName = "LEARNING"
clientCallback @ 0xF49F93C0
next = 0x9091D52C

clientID  = 24
clientSeq = 24
clientName = "PLATFORM-SPI"
clientCallback @ 0xF4AAD6F0
next = 0x91F2AE14

clientID  = 25
clientSeq = 25
clientName = "EEM"
clientCallback @ 0xF5393370
next = 0x913474F4

clientID  = 26
clientSeq = 26
clientName = "NG3K_WIRELESS"
clientCallback @ 0xF4B130B0
next = 0x9131D144

clientID  = 27
clientSeq = 27
clientName = "NG3K Environment Variables"
clientCallback @ 0xF4C6DA80
next = 0x00000000

KATANA_DOC#
KATANA_DOC#
KATANA_DOC#show platform ses clients
Client list @ 0x915B312C

clientID  = 0
clientSeq = 0
clientName = "TM Shim"
clientCallback @ 0xF4C79A90
next = 0x91182F24

clientID  = 1
clientSeq = 1
clientName = "EM-HA"
clientCallback @ 0xF52CA730
next = 0x913245B8

clientID  = 2
clientSeq = 2
clientName = "IFM"
clientCallback @ 0xF4A3EB20
next = 0x934B80E4

clientID  = 3
clientSeq = 3
clientName = "PORT-MGR"
clientCallback @ 0xF49FD0A0
next = 0x91D36D08

clientID  = 4
clientSeq = 4
clientName = "IDBMAN"
clientCallback @ 0xF4AF6040
next = 0x92121224

clientID  = 5
clientSeq = 5
clientName = "MATM"
```

```
clientCallback @ 0xF49F7300
next = 0x909194B4

clientID  = 6
clientSeq = 6
clientName = "L2 CONTROL"
clientCallback @ 0xF49CA3F0
next = 0x915E4E80

clientID  = 7
clientSeq = 7
clientName = "CDP"
clientCallback @ 0xF49C7220
next = 0x915E4F08

clientID  = 8
clientSeq = 8
clientName = "UDLD"
clientCallback @ 0xF49C75D0
next = 0x91854CA0

clientID  = 9
clientSeq = 9
clientName = "LLDP"
clientCallback @ 0xF49E62F0
next = 0x90919F90

clientID  = 10
clientSeq = 10
clientName = "L2M"
clientCallback @ 0xF49CE4D0
next = 0x90E35A5C

clientID  = 11
clientSeq = 11
clientName = "Storm-Control"
clientCallback @ 0xF4BA8080
next = 0x9089E9B4

clientID  = 12
clientSeq = 12
clientName = "Security Utils"
clientCallback @ 0xF466BFB0
next = 0x91855F14

clientID  = 13
clientSeq = 13
clientName = "BACKUP-INT"
clientCallback @ 0xF4A191B0
next = 0x91D3511C

clientID  = 14
clientSeq = 14
clientName = "SPAN"
clientCallback @ 0xF4A34F30
next = 0x90FFC8C8

clientID  = 15
clientSeq = 15
clientName = "NG3K_SES_CLIENT_SECURITY_CTRL"
clientCallback @ 0xF4CD1D80
next = 0x95AE5834

clientID  = 16
clientSeq = 16
clientName = "NG3K_SES_CLIENT_DAI"
clientCallback @ 0xF4CD0C50
next = 0x95AE4854

clientID  = 17
clientSeq = 17
clientName = "NG3K_SES_CLIENT_DHCPSN"
clientCallback @ 0xF4CA9D30
```

```
next = 0x91DF7728

clientID  = 18
clientSeq = 18
clientName = "NG3K_SES_CLIENT_IPSG"
clientCallback @ 0xF4CDED70
next = 0x9131DCD8

clientID  = 20
clientSeq = 20
clientName = "DTLS"
clientCallback @ 0xF49B2CB0
next = 0x9134508C

clientID  = 21
clientSeq = 21
clientName = "STATS"
clientCallback @ 0xF49BD750
next = 0x9134746C

clientID  = 22
clientSeq = 22
clientName = "PLATFORM_MGR"
clientCallback @ 0xF4AB2D40
next = 0x91323D20

clientID  = 23
clientSeq = 23
clientName = "LEARNING"
clientCallback @ 0xF49F93C0
next = 0x9091D52C

clientID  = 24
clientSeq = 24
clientName = "PLATFORM-SPI"
clientCallback @ 0xF4AAD6F0
next = 0x91F2AE14

clientID  = 25
clientSeq = 25
clientName = "EEM"
clientCallback @ 0xF5393370
next = 0x913474F4

clientID  = 26
clientSeq = 26
clientName = "NG3K_WIRELESS"
clientCallback @ 0xF4B130B0
next = 0x9131D144

clientID  = 27
clientSeq = 27
clientName = "NG3K Environment Variables"
clientCallback @ 0xF4C6DA80
next = 0x00000000
```

show platform stack-manager

プラットフォーム依存スイッチスタック情報を表示するには、特権EXECモードで**show platform stack-manager** コマンドを使用します。

show platform stack-manager {**oir-states**| **sdp-counters**| **sif-counters**} **switch** *stack-member-number*

構文の説明

oir-states	活性挿抜（OIR）状態の情報を表示します。

sdp-counters	スタック ディスカバリ プロトコル（SDP）カウンタ情報を表示します。
sif-counters	スタック情報（SIF）カウンタ情報を表示します。
switch *stack-member-number*	スタック マネージャ情報を表示するスタック メンバを指定します。

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
Cisco IOS XE 3.2SE	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 スタックのデータと統計を収集するには、**show platform stack-manager** コマンドを使用します。

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show redundancy

冗長ファシリティ情報を表示するには、特権 EXEC モードで **show redundancy** コマンドを使用します。

show redundancy [**clients**| **config-sync**| **counters**| **history** [**reload**| **reverse**]| **slaves**[*slave-name*] {**clients**| **counters**}| **states**| **switchover history** [**domain default**]]

構文の説明

clients	（任意）冗長ファシリティ クライアントに関する情報を表示します。

config-sync	（任意）コンフィギュレーション同期の失敗または無視されたMismatched Command List（MCL）を表示します。詳細については、show redundancy config-sync, （1202 ページ）を参照してください。
counters	（任意）冗長ファシリティ カウンタに関する情報を表示します。
history	（任意）冗長ファシリティの過去のステータスのログおよび関連情報を表示します。
history reload	（任意）冗長ファシリティの過去のリロード情報を表示します。
history reverse	（任意）冗長ファシリティの過去のステータスおよび関連情報のログを逆順で表示します。
slaves	（任意）冗長ファシリティのすべてのスレーブを表示します。
slave-name	（任意）特定の情報を表示する冗長ファシリティ スレーブの名前。指定スレーブのすべてのクライアントまたはカウンタを表示するには、追加でキーワードを入力します。
clients	指定スレーブのすべての冗長ファシリティ クライアントを表示します。
counters	指定スレーブのすべてのカウンタを表示します。
states	（任意）冗長ファシリティの状態（ディセーブル、初期化、スタンバイ、アクティブなど）に関する情報を表示します。
switchover history	（任意）冗長ファシリティのスイッチオーバー履歴に関する情報を表示します。
domain default	（任意）スイッチオーバー履歴を表示するドメインとしてデフォルト ドメインを表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、冗長ファシリティに関する情報を表示する方法を示します。

```
Device# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 6 days, 9 hours, 23 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = not known

                 Hardware Mode = Simplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Down      Reason: Simplex mode

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 6 days, 9 hours, 23 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 3
850 L3 Switch Software (CAT3850-UNIVERSALK9-M), Version 03.08.59.EMD EARLY DEPLO
YMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_11
05
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 16-S
        Configuration register = 0x102

Peer (slot: 0) information is not available because it is in 'DISABLED' state
Device#
```

次の例では、冗長ファシリティ クライアント情報を表示する方法を示します。

```
Device# show redundancy clients
Group ID =     1
     clientID = 20002    clientSeq =     4    EICORE HA Client
     clientID = 24100    clientSeq =     5    WCM_CAPWAP
     clientID = 24101    clientSeq =     6    WCM_RRM HA
     clientID = 24103    clientSeq =     8    WCM_QOS HA
     clientID = 24105    clientSeq =    10    WCM_MOBILITY
     clientID = 24106    clientSeq =    11    WCM_DOT1X
     clientID = 24107    clientSeq =    12    WCM_APFROGUE
     clientID = 24110    clientSeq =    15    WCM_CIDS
     clientID = 24111    clientSeq =    16    WCM_NETFLOW
     clientID = 24112    clientSeq =    17    WCM_MCAST
     clientID = 24120    clientSeq =    18    wcm_comet
     clientID = 24001    clientSeq =    21    Table Manager Client
     clientID = 20010    clientSeq =    24    SNMP SA HA Client
     clientID = 20007    clientSeq =    27    Installer HA Client
     clientID =    29    clientSeq =    60    Redundancy Mode RF
     clientID =   139    clientSeq =    61    IfIndex
     clientID =  3300    clientSeq =    62    Persistent Variable
     clientID =    25    clientSeq =    68    CHKPT RF
     clientID = 20005    clientSeq =    74    IIF-shim
     clientID = 10001    clientSeq =    82    QEMU Platform RF

<output truncated>
```

出力には、次の情報が表示されます。

- clientID には、クライアントの ID 番号が表示されます。
- clientSeq には、クライアントの通知シーケンス番号が表示されます。
- 現在の冗長ファシリティ ステート。

次の例では、冗長ファシリティ カウンタ情報を表示する方法を示します。

```
Device# show redundancy counters
Redundancy Facility OMs

               comm link up = 0
             comm link down = 0
          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
         errored peer msg rx = 0

                 buffers tx = 0
     tx buffers unavailable = 0
                 buffers rx = 0
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0

Device#
```

次の例では、冗長ファシリティ履歴情報を表示する方法を示します。

```
Device# show redundancy history
00:00:00 *my state = INITIALIZATION(2) peer state = DISABLED(1)
00:00:00 RF_EVENT_INITIALIZATION(524) op=0 rc=0
00:00:00 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:01 client added: Table Manager Client(24001) seq=21
00:00:01 client added: SNMP SA HA Client(20010) seq=24
00:00:06 client added: WCM_CAPWAP(24100) seq=5
00:00:06 client added: WCM_QOS HA(24103) seq=8
00:00:07 client added: WCM_DOT1X(24106) seq=11
00:00:07 client added: EICORE HA Client(20002) seq=4
00:00:09 client added: WCM_MOBILITY(24105) seq=10
00:00:09 client added: WCM_NETFLOW(24111) seq=16
00:00:09 client added: WCM_APFROGUE(24107) seq=12
00:00:09 client added: WCM_RRM HA(24101) seq=6
00:00:09 client added: WCM_MCAST(24112) seq=17
00:00:09 client added: WCM_CIDS(24110) seq=15
00:00:09 client added: wcm_comet(24120) seq=18
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) First Slave(0) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6107) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6109) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6128) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8897) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8898) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8901) op=0 rc=0
00:00:22 RF_EVENT_SLAVE_STATUS_DONE(523) First Slave(0) op=405 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Redundancy Mode RF(29) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) IfIndex(139) op=0 rc=0

<output truncated>
```

次の例では、冗長ファシリティ スレーブに関する情報を表示する方法を示します。

```
Device# show redundancy slaves
Group ID =   1
Slave/Process ID =  6107   Slave Name = [installer]
Slave/Process ID =  6109   Slave Name = [eicored]
Slave/Process ID =  6128   Slave Name = [snmp_subagent]
Slave/Process ID =  8897   Slave Name = [wcm]
Slave/Process ID =  8898   Slave Name = [table_mgr]
Slave/Process ID =  8901   Slave Name = [iosd]
```

```
Device#
```

次の例では、冗長ファシリティ ステートに関する情報を表示する方法を示します。

```
Device# show redundancy states
         my state = 13 -ACTIVE
       peer state =  1 -DISABLED
            Mode = Simplex
         Unit ID = 1

  Redundancy Mode (Operational) = SSO
   Redundancy Mode (Configured) = SSO
              Redundancy State = Non Redundant
                    Manual Swact = disabled (system is simplex (no peer unit))

   Communications = Down      Reason: Simplex mode

     client count = 75
   client_notification_TMR = 360000 milliseconds
            keep_alive TMR = 9000 milliseconds
          keep_alive count = 0
      keep_alive threshold = 18
             RF debug mask = 0

Device#
```

show redundancy config-sync

コンフィギュレーション同期障害情報または無視されたMismatched Command List（MCL）（存在する場合）を表示するには、EXECモードで**show redundancy config-sync**コマンドを使用します。

show redundancy config-sync {**failures** {**bem| mcl| prc**}| **ignored failures mcl**}

構文の説明

failures	MCLエントリまたはベストエフォート方式（BEM）/パーサーリターンコード（PRC）の障害を表示します。
bem	BEM障害コマンドリストを表示し、スタンバイ スイッチを強制的にリブートします。
mcl	スイッチの実行コンフィギュレーションに存在するがスタンバイ スイッチのイメージでサポートされていないコマンドを表示し、スタンバイ スイッチを強制的にリブートします。
prc	PRC障害コマンドリストを表示し、スタンバイ スイッチを強制的にリブートします。
ignored failures mcl	無視されたMCL障害を表示します。

コマンドモード

なし ザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 つのバージョンの Cisco IOS イメージが含まれている場合は、それぞれのイメージによってサポートされるコマンドセットが異なる可能性があります。このような不一致コマンドのいずれかがアクティブスイッチで実行された場合、スタンバイスイッチでそのコマンドを認識できない可能性があり、これにより設定の不一致状態が発生します。バルク同期中にスタンバイ スイッチでコマンドの構文チェックが失敗すると、コマンドはMCLに移動し、スタンバイ スイッチはリセットされます。すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブ スイッチの実行コンフィギュレーションから、不一致コマンドをすべて削除します。
2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイ スイッチをリロードします。

または、次の手順を実行して MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイ スイッチをリロードします。システムは SSO モードに遷移します。

（注） 不一致コマンドを無視する場合、アクティブ スイッチとスタンバイ スイッチの同期していないコンフィギュレーションは存在したままです。

3. 無視した MCL は **show redundancy config-sync ignored mcl** コマンドで確認できます。

各コマンドでは、そのコマンドを実装するアクション機能において戻りコードが設定されます。この戻りコードは、コマンドが正常に実行されたかどうかを示します。アクティブ スイッチは、コマンドの実行後に PRC を維持します。スタンバイ スイッチはコマンドを実行し、アクティブスイッチに PRC を返します。これら 2 つの PRC が一致しないと、PRC 障害が発生します。バルク同期または 1 行ごとの（LBL）同期中にスタンバイ スイッチで PRC エラーが生じた場合、スタンバイ スイッチはリセットされます。すべての PRC 障害を表示するには、**show redundancy config-sync failures prc** コマンドを使用します。

ベストエフォート方式（BEM）エラーを表示するには、**show redundancy config-sync failures bem** コマンドを使用します。

次に、BEM 障害を表示する例を示します。

```
Device> show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

 The list is Empty
```

次に、MCL 障害を表示する例を示します。

```
Device> show redundancy config-sync failures mcl
Mismatched Command List
-----------------------

The list is Empty
```

次に、PRC 障害を表示する例を示します。

```
Device# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------

 The list is Empty
```

show switch

スタック メンバまたはスイッチ スタックに関連した情報を表示するには、**show switch** コマンドを EXEC モードで使用します。

show switch [*stack-member-number*| **detail**| **neighbors**| **stack-ports** [**summary**]]

構文の説明

stack-member-number	（任意）スタック メンバ数。指定できる範囲は 1 ～ 9 です。
detail	（任意）スタック リングの詳細情報を表示します。
neighbors	（任意）スイッチスタック全体のネイバーを表示します。
stack-ports	（任意）スイッチスタック全体のポート情報を表示します。
summary	（任意）スタック ケーブルの長さ、スタック リンクのステータス、およびループバックのステータスを表示します。

コマンド ヂヲボルト

なセザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、次のステートが表示されます。

- Initializing：スイッチはスタックに追加されたばかりで、ready 状態になるための基本的な初期化が完了していません。
- HA Sync in Progress：スタンバイが選出されると、同期が終了するまで対応するスイッチはこの状態のままになります。
- Syncing：既存のスタックに追加されたスイッチは、スイッチ追加シーケンスが完了するまでこの状態のままになります。
- Ready：メンバがシステム レベルおよびインターフェイス レベルの設定のロードを完了し、トラフィックを転送できるようになっています。
- V-Mismatch：Version-Mismatch モードのスイッチ。Version-Mismatch モードは、スタックに参加したスイッチのソフトウェア バージョンがアクティブ スイッチと非互換である場合です。
- Provisioned：スイッチ スタックのアクティブ メンバになる前にすでに設定されていたスイッチの状態です。プロビジョニングされたスイッチでは、MACアドレスおよびプライオリティ番号は、常に 0 と表示されます。
- Unprovisioned：プロビジョニングされたスイッチ番号が **no switch** *switch-number* **provision** コマンドを使用してプロビジョニング解除された場合の状態です。
- Removed：スタックに存在していたスイッチが、**reload slot** コマンドを使用して除外された場合です。
- Sync not started：複数のスイッチが既存のスタックに同時に追加された場合、アクティブ スイッチが 1 台ずつ追加します。追加中のスイッチは Syncing 状態になります。まだ追加されていないスイッチは Sync not started 状態になります。
- Lic-Mismatch：スイッチのライセンス レベルがアクティブ スイッチと異なります。

スタック メンバ（アクティブ スイッチを含む）の代表的なステート遷移は、Waiting > Initializing > Ready です。

Version Mismatch（VM）モードのスタック メンバの代表的なステート遷移は、Waiting > Ver Mismatch です。

スイッチスタックにプロビジョニングされたスイッチが存在するかどうかを識別するには、**show switch** コマンドを使用できます。**show running-config** および **show startup-config** 特権 EXEC コマンドでは、この情報は提供されません。

永続的 MAC アドレスがイネーブルになっている場合、スタックの MAC-persistency wait-time も表示されます。

次に、スタック情報の概要を表示する例を示します。

```
Device# show switch
Switch/Stack Mac Address : 6400.f124.e900
                                            H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------
 1       Member   0000.0000.0000     0       0       Provisioned
 2       Member   0000.0000.0000     0       0       Removed
*3       Active   6400.f124.e900     2       0       Ready
 8       Member   0000.0000.0000     0       0       Unprovisioned
```

次に、スタック情報の詳細を表示する例を示します。

```
Device# show switch detail
Switch/Stack Mac Address : 2037.06ce.3f80 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Active 2037.06ce.3f80     1       0       Ready
 2       Member 0000.000.0000      0       0       Provisioned
 6       Member 2037.06ce.1e00     1       0       Ready

           Stack Port Status             Neighbors
Switch#   Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
  1       Ok         Down             6        None
  6       Down       Ok               None       1
```

次に、メンバ 6 の要約情報を表示する例を示します。

```
Device# show switch 6
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------------
 6       Member     0003.e31a.1e00     1          Ready
```

次に、スタックに関するネイバー情報を表示する例を示します。

```
Device# show switch neighbors
  Switch #    Port A       Port B
  --------    ------       ------
      6        None           8
      8         6            None
```

次に、スタック ポート情報を表示する例を示します。

```
Device# show switch stack-ports
  Switch #    Port A       Port B
  --------    ------       ------
    6          Down          Ok
    8           Ok           Down
```

次に、**show switch stack-ports summary** コマンドの出力例を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device# show switch stack-ports summary
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
          Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     Down      2       50 cm     No     NO      No      10         No
```

```
1/2     Ok        3       1 m       Yes    Yes     Yes     0          No
2/1     Ok        5       3 m       Yes    Yes     Yes     0          No
2/2     Down      1       50 cm     No     No      No      10         No
3/1     Ok        1       1 m       Yes    Yes     Yes     0          No
3/2     Ok        5       1 m       Yes    Yes     Yes     0          No
5/1     Ok        3       1 m       Yes    Yes     Yes     0          No
5/2     Ok        2       3 m       Yes    Yes     Yes     0          No
```

表 *46*：*show switch stack-ports summary* コマンドの出力

フィールド	説明
Switch#/Port#	メンバー番号と、そのスタック ポート番号
Stack Port Status	スタック ポートのステータス。 • Absent：スタック ポートにケーブルが検出されません。 • Down：ケーブルは検出されましたが、接続されたネイバーがアップになっていないか、スタック ポートがディセーブルになっています。 • OK：ケーブルが検出され、接続済みのネイバーが起動しています。
Neighbor	スタック ケーブルの接続先の、アクティブなメンバーのスイッチの数。
Cable Length	有効な長さは 50 cm、1 m、または 3 m です。 スイッチがケーブルの長さを検出できない場合は、値は *no cable* になります。ケーブルが接続されていないか、リンクが信頼できない可能性があります。
Link OK	スタック ケーブルが接続され機能しているかどうか。相手側には、接続されたネイバーが存在する場合も、そうでない場合もあります。 リンク パートナーは、ネイバー スイッチ上のスタック ポートのことです。 • No：このポートに接続されているスタック ケーブルがないか、スタック ケーブルが機能していません。 • Yes：このポートには正常に機能するスタック ケーブルが接続されています。

フィールド	説明
Link Active	スタック ケーブル相手側にネイバーが接続されているかどうか。 • No：相手側にネイバーが検出されません。ポートは、このリンクからトラフィックを送信できません。 • Yes：相手側にネイバーが検出されました。ポートは、このリンクからトラフィックを送信できます。
Sync OK	リンク パートナーが、スタック ポートに有効なプロトコル メッセージを送信するかどうか。 • No：リンク パートナーからスタック ポートに有効なプロトコル メッセージが送信されません。 • Yes：リンクの相手側は、ポートに有効なプロトコル メッセージを送信します。
# Changes to LinkOK	リンクの相対的安定性。 短期間で多数の変更が行われた場合は、リンクのフラップが発生することがあります。
In Loopback	スタック ケーブルがメンバのスタック ポートに接続されているかどうか。 • No：メンバ上の少なくとも 1 つのスタック ポートに接続済みのスタック ケーブルがあります。 • Yes：メンバーのどのスタック ポートにも、スタック ケーブルが接続されていません。

関連トピック

reload, （1179 ページ）

session, （1180 ページ）

stack-mac update force, （1212 ページ）

switch priority, （1216 ページ）

switch provision, （1217 ページ）
switch renumber, （1219 ページ）

show trace messages capwap ap ha

ワイヤレス Control And Provisioning of Wireless Access Points（CAPWAP）ハイ アベイラビリティを表示するには、**show trace messagescapwap ap ha** 特権 EXEC コマンドを使用します。

show trace messages capwap ap ha [**detail**| **event**| **dump**] [**switch** *switch*]

構文の説明

detail	（任意）ワイヤレス CAPWAP ハイ アベイラビリティの詳細を表示します。
detail*switch number*	デバイス番号を指定します。値は 1 です。
event	（任意）ワイヤレス CAPWAP ハイ アベイラビリティのイベントを表示します。
event*switch number*	デバイス番号を指定します。値は 1 です。
dump	（任意）ワイヤレス CAPWAP ハイ アベイラビリティの出力を表示します。
dump *switch number*	デバイス番号を指定します。値は 1 です。
switch	（任意）デバイス番号を表示します。値は 1 です。
switch *switch number*	デバイス番号を指定します。値は 1 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、CAPWAP ハイ アベイラビリティ出力を表示する例を示します。

```
Device# show trace messages mobility ha dump switch 1
|  Output modifiers
  <cr>
```

show trace messages mobility ha

ワイヤレス モビリティ ハイ アベイラビリティを表示するには、**show trace messages mobility ha** 特権 EXEC コマンドを使用します。

show trace messages mobility ha [**event**| **detail**| **dump**] [**switch** *switch*]

構文の説明

event	（任意）ワイヤレス モビリティ HA のイベントを表示します。
event*switch*	デバイス番号を指定します。値は 1 です。
detail	（任意）ワイヤレス モビリティ HA の詳細を表示します。
detail*switch*	デバイス番号を指定します。値は 1 です。
dump	（任意）ワイヤレス モビリティ HA の出力デバッグを表示します。
dump*switch*	デバイス番号を指定します。値は 1 です。
switch*switch*	（任意）デバイス番号を表示します。
switch*switch*	デバイス番号を指定します。値は 1 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ワイヤレス モビリティ ハイ アベイラビリティを表示する例を示します。

```
Device# show trace messages mobility ha
```

stack-mac persistent timer

固定 MAC アドレス機能をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチのグローバル コンフィギュレーション モードで **stack-mac persistent timer** コマンドを使用します。固定 MAC アドレ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。

stack-mac persistent timer [**0**| *time-value*]

no stack-mac persistent timer

構文の説明

0	（任意）現在のアクティブ スイッチの MAC アドレスの使用を無期限に継続し、新しいアクティブ スイッチが引き継いだ場合もそうします。
time-value	（任意）スタック MAC アドレスが新しい アクティブ スイッチ の MAC アドレスに変わるまでの時間（分単位）。指定できる範囲は 1 ～ 60 分です。

コマンド デフォルト

固定 MAC アドレスはディセーブルに設定されています。スタックの MAC アドレスは常に、アクティブ スイッチ の MAC アドレスです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、新しいアクティブ スイッチが引き継ぐ場合でも、スタック MAC アドレスは最初のアクティブ スイッチの MAC アドレスになります。同じ動作は、**stack-mac persistent timer** コマンドまたは **stack-mac persistent timer 0** コマンドを入力した場合にも発生します。

stack-mac persistent timer コマンドを *time-value* とともに入力すると、新しいスイッチがアクティブ スイッチになったときに、入力した時間の後にスタック MAC アドレスが新しいアクティブ スイッチのものに変わります。以前のアクティブ スイッチがこの時間内にスタックに再加入した場合、スタックはその MAC アドレスを持つスイッチがスタック内に存在する限り、その MAC アドレスを保持します。

スタック全体をリロードすると、アクティブ スイッチの MAC アドレスがスタックの MAC アドレスになります。

（注） スタック MAC アドレスを変更しない場合、レイヤ 3 インターフェイスのフラップが発生しません。これは、未知の MAC アドレス（スタック内のスイッチに属さない MAC アドレス）がスタック MAC アドレスになる可能性があることを意味します。この未知の MAC アドレスを持つスイッチが別のスタックにアクティブ スイッチとして参加すると、2 つのスタックが同じスタック MAC アドレスを持つことになります。**stack-mac update force** コマンドを使用して、この競合を解決する必要があります。

次に、固定 MAC アドレスをイネーブルにする例を示します。

```
Device(config)# stack-mac persistent timer
```

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。イネーブルの場合、出力に **stack-mac persistent timer** が表示されます。

関連トピック

stack-mac update force, （1212 ページ）

stack-mac update force

スタック MAC アドレスをアクティブ スイッチの MAC アドレスに更新するには、アクティブ スイッチの EXEC モードで **stack-mac update force** コマンドを使用します。

stack-mac update force

構文の説明

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

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、ハイ アベイラビリティ（HA）フェールオーバー時に、スタックのMACアドレスは新しいアクティブ スイッチのMACアドレスに変更されません。スタック MAC アドレスが新しいアクティブ スイッチの MAC アドレスに強制的に変更されるようにするには、**stack-mac update force** コマンドを使用します。

スタックMACアドレスと同じMACアドレスを持つスイッチが現在そのスタックのメンバーである場合、**stack-mac update force** コマンドは無効です。（スタック MAC アドレスはアクティブ スイッチの MAC アドレスに更新されません）

（注） スタック MAC アドレスを変更しない場合、レイヤ 3 インターフェイスのフラップが発生しません。これは、未知の MAC アドレス（スタック内のスイッチに属さない MAC アドレス）がスタック MAC アドレスになる可能性があることを意味します。この未知の MAC アドレスを持つスイッチが別のスタックにアクティブ スイッチとして参加すると、2つのスタックが同じスタック MAC アドレスを持つことになります。**stack-mac update force** コマンドを使用して、この競合を解決する必要があります。

次に、スタックMACアドレスをアクティブ スイッチのMACアドレスに更新する例を示します。

```
Device> stack-mac update force
Device>
```

設定を確認するには、**show switch** 特権 EXEC コマンドを入力します。スタック MAC アドレスには、MAC アドレスがローカルと未知のどちらであるかも含まれます。

関連トピック

show switch, （1204 ページ）

stack-mac persistent timer, （1211 ページ）

standby console enable

スタンバイ コンソール スイッチへのアクセスを有効にするには、冗長メイン コンフィギュレーション サブモードで **standby console enable** コマンドを使用します。スタンバイ コンソール スイッチへのアクセスを無効にするには、このコマンドの **no** 形式を使用します。

standby console enable

no standby console 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

スタンバイ スイッチ コンソールへのアクセスはディセーブルです。

コマンド モード

冗長メイン コンフィギュレーション サブモード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、スタンバイ コンソールに関する特定のデータを収集し、確認するために使用されます。コマンドは、主に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ちます。

次に、冗長メイン コンフィギュレーション サブモードを開始し、スタンバイ コンソール スイッチへのアクセスをイネーブルにする例を示します。

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)#
```

関連トピック

main-cpu, （1171 ページ）

switch stack port

メンバの指定されたスタック ポートをディセーブルまたはイネーブルにするには、スタック メンバの特権 EXEC モードで **switch** コマンドを使用します。

switch *stack-member-number* **stack port** *port-number* {**disable| enable**}

構文の説明

stack-member-number	現在のスタック メンバ番号。指定できる範囲は 1 ～ 9 です。

stackport*port-number*	メンバ上のスタック ポートを指定します。指定できる範囲は 1 ～ 2 です。
disable	指定したポートをディセーブルにします。
enable	指定されたポートをイネーブルにします。

コマンド デフォルト

スタック ポートはイネーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

スタックが full-ring 状態になるのは、すべてのスタック メンバがスタック ポートを使用して接続され、ready 状態になっている場合です。

スタックが partial-ring 状態になるのは、次が発生したときです。

- すべてのメンバがスタック ポートを通じて接続されたが、一部が ready ステートではない。
- スタック ポートを通じて接続されていないメンバーがある。

（注） **switch***stack-member-number***stackport***port-number***disable** コマンドの使用には注意が必要です。スタック ポートをディセーブルにすると、スタックは半分の帯域幅で稼働します。

switch*stack-member-number***stackport***port-number***disable** 特権 EXEC コマンドを入力し、スタックが full-ring 状態にある場合、ディセーブルにできるスタック ポートは 1 つだけです。次のメッセージが表示されます。

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

switch *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力し、スタックが partial-ring 状態にある場合、ポートはディセーブルにできません。次のメッセージが表示されます。

```
Disabling stack port not allowed with current stack configuration.
```

次に、member 4 上の stack port 2 をディセーブルにする方法の例を示します。

```
Device# switch 4 stack port 2 disable
```

関連トピック

show switch, （1204 ページ）

switch priority

スタック メンバーのプライオリティ値を変更するには、アクティブ スイッチの EXEC モードで **switch priority** コマンドを使用します。

switch *stack-member-number* **priority** *new-priority-value*

構文の説明

stack-member-number	現在のスタック メンバ番号。指定できる範囲は 1 ～ 9 です。
new-priority-value	スタック メンバの新しいプライオリティ値指定できる範囲は 1 ～ 15 です。

コマンド デフォルト

デフォルトのプライオリティ値は 1 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

新しいプライオリティ値は、新しいアクティブ スイッチ選定の要素になります。プライオリティ値を変更しても、アクティブ スイッチ がただちに変更されることはありません。

次の例では、スタック メンバ 6 のプライオリティ値を 8 に変更する方法を示します。

```
Device# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

関連トピック

reload, （1179 ページ）

session, （1180 ページ）

show switch, （1204 ページ）

switch renumber, （1219 ページ）

switch provision

新しいスイッチがスイッチスタックに追加される前に構成設定するには、アクティブスイッチのグローバル コンフィギュレーション モードで **switch provision** コマンドを使用します。除外されたスイッチ（スタックを離れたスタック メンバ）に対応するすべての設定情報を削除するには、このコマンドの **no** 形式を使用します。

switch *stack-member-number* **provision** *type*

no switch *stack-member-number* **provision**

構文の説明

stack-member-number	スタック メンバの番号です。指定できる範囲は 1 ～ 9 です。
type	新しいスイッチがスタックに加入する前の、このスイッチのタイプ。

コマンド デフォルト

スイッチは、プロビジョニングされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

type には、コマンドライン ヘルプ ストリングに示されたサポート対象のスイッチのモデル番号を入力します。

エラー メッセージを受信しないようにするには、このコマンドの **no** 形式を使用してプロビジョニングされた設定を削除する前に、スイッチ スタックから指定のスイッチを削除する必要があります。

スイッチタイプを変更する場合も、スイッチスタックから指定のスイッチを削除する必要があります。スイッチ タイプを変更しない場合でも、スイッチ スタック内に物理的に存在するプロビジョニングされたスイッチのスタック メンバ番号を変更できます。

プロビジョニングされたスイッチのタイプが、スタック上のプロビジョニングされた設定のスイッチタイプと一致しない場合、スイッチスタックはプロビジョニングされたスイッチにデフォルト設定を適用し、これをスタックに追加します。スイッチ スタックでは、デフォルト設定を適用する場合にメッセージを表示します。

プロビジョニング情報は、スイッチ スタックの実行コンフィギュレーションで表示されます。**copy running-config startup-config** 特権 EXEC コマンドを入力すると、プロビジョニングされた設定がスイッチ スタックのスタートアップ コンフィギュレーション ファイルに保存されます。

注意 **switch provision** コマンドを使用すると、プロビジョニングされた設定にメモリが割り当てられます。新しいスイッチ タイプが設定されたときに、以前割り当てられたメモリのすべてが解放されるわけではありません。そのため、このコマンドをおおよそ200回を超えて使用しないようにしてください。スイッチのメモリが不足し、予期せぬ動作が発生する可能性があります。

次に、スタック メンバー番号2が設定されたスイッチをスイッチ スタックに割り当てる例を示します。**show running-config** コマンドの出力は、プロビジョニングされたスイッチに関連付けられたインターフェイスを示します。

```
Device(config)# switch 2 provision WS-xxxx
Device(config)# end
Device# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

また、**show switch** ユーザ EXEC コマンドを入力すると、スイッチ スタックのプロビジョニングされたステータスを表示できます。

次の例では、スイッチがスタックから削除される場合に、スタック メンバ 5 についてのすべての設定情報が削除される方法を示します。

```
Device(config)# no switch 5 provision
```

プロビジョニングされたスイッチが、実行コンフィギュレーションで追加または削除されたことを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連トピック

show switch, （1204 ページ）

switch renumber

スタック メンバ番号を変更するには、**switch renumber** コマンドを アクティブ スイッチ の EXEC モードで使用します。

switch *current-stack-member-number* **renumber** *new-stack-member-number*

構文の説明

current-stack-member-number	現在のスタック メンバ番号。指定できる範囲は1～9です。
new-stack-member-number	スタック メンバの新しいスタック メンバ番号。指定できる範囲は 1 ～ 9 です。

コマンド デフォルト

デフォルトのスタック メンバ番号は 1 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

指定したメンバ番号をすでに他のスタック メンバが使用している場合、スタック メンバをリロードする際に アクティブ スイッチ は使用可能な一番低い番号を割り当てます。

（注） スタック メンバ番号を変更し、新しいスタック メンバ番号がどの設定にも関連付けされていない場合、そのスタック メンバは現在の設定を廃棄してリセットを行い、デフォルトの設定に戻ります。

プロビジョニングされたスイッチでは、**switch***current-stack-member-number***renumber***new-stack-member-number* コマンドを使用しないでください。使用すると、コマンドは拒否されます。

スタック メンバをリロードし、設定変更を適用するには、**reload slot***current stack member number* 特権 EXEC コマンドを使用します。

次の例では、スタック メンバ 6 のメンバ番号を 7 に変更する方法を示しています。

```
Device# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a provisioned
 configuration.
Do you want to continue?[confirm]
```

関連トピック

reload, （1179 ページ）

session, （1180 ページ）

show switch, （1204 ページ）

switch priority, （1216 ページ）

第 20 章

StackWise Virtual コマンド

- stackwise-virtual, 1221 ページ
- domain id, 1222 ページ
- stackwise-virtual link , 1223 ページ
- stackwise-virtual dual-active-detection, 1224 ページ
- show stackwise-virtual, 1225 ページ

stackwise-virtual

スイッチの Cisco StackWise Virtual を有効にするには、グローバル コンフィギュレーション モードで **stackwise-virtual** コマンドを使用します。Cisco StackWise Virtual を無効にするには、このコマンドの **no** 形式を使用します。

stackwise-virtual

no stackwise-virtual

構文の説明

stackwise-virtual	Cisco StackWise Virtual を有効にします。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.3	このコマンドが導入されました。

使用上のガイドライン

Cisco StackWise Virtual を無効にしたら、スイッチをリロードしてスタック解除する必要があります。

例

次に、Cisco StackWise Virtual を有効にする例を示します。

```
Device(config)# stackwise-virtual
```

domain id

スイッチで Cisco StackWise Virtual ドメイン ID を設定するには、StackWise Virtual コンフィギュレーション モードで **domain** *id* コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します。

domain *id*

no domain *id*

構文の説明

domain	StackWise Virtual 設定を特定のドメインに関連付けます。
id	ドメイン ID の値。範囲は 1 ～ 255 です。デフォルトは 1 です。

コマンド デフォルト

ドメイン ID が設定されていません。

コマンド モード

StackWise Virtual コンフィギュレーション（config-stackwise-virtual）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.3	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションです。ドメイン ID を設定する前に、**stackwise-virtual** コマンドを使用して StackWise Virtual を有効にする必要があります。

例

次に、Cisco StackWise Virtual を有効にして、ドメイン ID を設定する例を示します。

```
Device(config)# stackwise-virtual
Device(config-stackwise-virtual)#domain 2
```

stackwise-virtual link

インターフェイスを設定済みの StackWise Virtual リンクと関連付けるには、インターフェイス コンフィギュレーション モードで **stackwise-virtual link** コマンドを使用します。インターフェイス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。

stackwise-virtual link *link-value*

no stackwise-virtual link *link-value*

構文の説明

stackwise-virtual link	StackWise Virtual リンクに 10 G または 40 G インターフェイスを関連付けます。
link value	Cisco StackWise Virtual に対して設定されているドメイン ID。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション（config-if）。

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.3	このコマンドが導入されました。

使用上のガイドライン

StackWise Virtual リンクは、10 G インターフェイスのポート値の範囲（45 ～ 48）、およびすべての 40 G インターフェイスでサポートされます。

例：

次に、40 ギガビット イーサネット インターフェイスと設定済みの Stackwise Virtual Link（SVL）を関連付ける例を示します。

```
Device(config)# interface FortyGigabitEthernet1/1/1
Device(config-if)#stackwise-virtual link 1
```

stackwise-virtual dual-active-detection

インターフェイスをデュアルアクティブ検出リンク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 **stackwise-virtual dual-active-detection** コマンドを使用します。インターフェイス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。

stackwise-virtual dual-active-detection

no stackwise-virtual dual-active-detection

構文の説明

stackwise-virtual dual-active-detection	指定された 10 G または 40 G インターフェイスの Cisco StackWise Virtual デュアル アクティブ検出を有効にします。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.3	このコマンドが導入されました。

例：

次に、10 ギガビット イーサネット インターフェイスをデュアル アクティブ検出リンクとして設定する例を示します。

```
Device(config)# interface TenGigabitEthernet1/0/2
Device(config-if)#stackwise-virtual dual-active-detection
```

show stackwise-virtual

Cisco StackWise Virtual の設定情報を表示するには、**show stackwise-virtual** コマンドを使用します。

show stackwise-virtual {[**switch** [*switch number <1-2>*] {**link**| **bandwidth**| **neighbors**| **dual-active-detection**}}

構文の説明

switch*number*	（任意）スタック内の特定のスイッチの情報を表示します。
link	Stackwise Virtual リンク情報を表示します。
bandwidth	Stackwise Virtual の帯域幅の可用性を表示します。
neighbors	Stackwise Virtual のネイバーを表示します。
dual-active-detection	Stackwise Virtual のデュアル アクティブ検出情報を表示します。

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
Cisco IOS XE Denali 16.3.3	このコマンドが導入されました。

例：

次に、**show stackwise-virtual** コマンドの出力例を示します。

```
Device#  show stackwise-virtual

Stackwise Virtual: <Enabled/Disabled>
Domain Number:     <Domain Number>
Switch    Stackwise Virtual Link     Ports
--------- ------------------------- --------------------------
1           1                        Tengigabitethernet1/0/4
            2                        Tengigabitethernet1/0/5
2           1                        Tengigabitethernet2/0/4
            2                        Tengigabitethernet2/0
```

次に、**show stackwise-virtual link** コマンドの出力例を示します。

```
Device# show stackwise-virtual link

Stackwise Virtual Link (SVL) Information:
-----------------------------------------------
Flags:
------
Link Status
--------------
U-Up D-Down
Protocol Status
------------------
S-Suspended P-Pending E-Error T-Timeout R-Ready
-----------------------------------------------------------------
Switch   SVL      Ports                          Link-Status      Protocol-Status
------   ---      -----                          -----------      ---------------
1        1        FortyGigabitEthernet1/1/1       U                R
2        1        FortyGigabitEthernet2/1/1       U                R
```

次に、**show stackwise-virtual bandwidth** コマンドの出力例を示します。

```
Device# show stackwise-virtual bandwidth

Switch  Bandwidth

1             160
2       160
```

次に、**show stackwise-virtual neighbors** コマンドの出力例を示します。

```
Device#show stackwise-virtual neighbors

Switch Number           Local Interface               Remote Interface

1                       Tengigabitethernet1/0/1  Tengigabitethernet2/0/1
                  Tengigabitethernet1/0/2  Tengigabitethernet2/0/2
2                 Tengigabitethernet2/0/1  Tengigabitethernet1/0/1
                  Tengigabitethernet2/0/2  Tengigabitethernet2/0/2
```

次に、**show stackwise-virtual dual-active-detection** コマンドの出力例を示します。

```
Device#show stackwise-virtual dual-active-detection

Stackwise Virtual Dual-Active-Detection (DAD) Configuration:
Switch Number       Dual-Active-Detection Interface
```

```
1                   Tengigabitethernet1/0/10
                    Tengigabitethernet1/0/11
2                   Tengigabitethernet2/0/12
                    Tengigabitethernet2/0/13

Stackwise Virtual Dual-Active-Detection (DAD) Configuration After Reboot:
Switch Number       Dual-Active-Detection Interface

1                   Tengigabitethernet1/0/10
                    Tengigabitethernet1/0/11
2                   Tengigabitethernet2/0/12
                    Tengigabitethernet2/0/13
```

第 XIX 部

システム管理

- システム管理コマンド，1231 ページ
- 自律型ネットワーキング コマンド，1361 ページ
- トレース コマンド，1375 ページ

第 21 章

システム管理コマンド

- ap hyperlocation, 1234 ページ
- ap name hyperlocation, 1235 ページ
- hyperlocation, 1236 ページ
- ap ntp ip, 1237 ページ
- ntp ip, 1238 ページ
- arp, 1239 ページ
- boot, 1240 ページ
- cat, 1241 ページ
- clear location, 1242 ページ
- clear location statistics, 1243 ページ
- clear nmsp statistics, 1244 ページ
- clear wireless ccx statistics, 1244 ページ
- clear wireless client tsm dot11, 1245 ページ
- clear wireless location s69 statistics, 1246 ページ
- copy, 1247 ページ
- config-ble, 1248 ページ
- copy startup-config tftp:, 1249 ページ
- copy tftp: startup-config, 1250 ページ
- debug call-admission wireless all, 1251 ページ
- debug rfid, 1252 ページ
- debug voice diagnostics mac-address, 1253 ページ

- debug wps mfp, 1253 ページ
- delete, 1254 ページ
- dir, 1255 ページ
- emergency-install, 1257 ページ
- exit, 1259 ページ
- flash_init, 1260 ページ
- help, 1260 ページ
- license right-to-use, 1261 ページ
- location, 1263 ページ
- location algorithm, 1267 ページ
- location expiry, 1268 ページ
- location notify-threshold, 1269 ページ
- location plm calibrating, 1270 ページ
- location rfid, 1271 ページ
- location rssi-half-life, 1272 ページ
- mac address-table move update, 1273 ページ
- mgmt_init, 1274 ページ
- mkdir, 1275 ページ
- more, 1276 ページ
- nmsp notification interval, 1277 ページ
- no debug all, 1278 ページ
- rename, 1279 ページ
- reset, 1280 ページ
- rmdir, 1281 ページ
- sdm prefer, 1282 ページ
- セット, 1283 ページ
- show avc client, 1286 ページ
- show avc wlan, 1287 ページ
- show cable-diagnostics tdr, 1288 ページ
- show ap hyperlocation, 1291 ページ
- show ap name hyperlocation, 1292 ページ

- show ap group ap-group-name hyperlocation, 1293 ページ
- show debug, 1294 ページ
- show env, 1295 ページ
- show env xps, 1297 ページ
- show flow monitor, 1301 ページ
- show license right-to-use, 1306 ページ
- show location, 1308 ページ
- show location ap-detect, 1309 ページ
- show mac address-table move update, 1310 ページ
- show nmsp, 1311 ページ
- show platform integrity, 1312 ページ
- show platform sudi certificate, 1313 ページ
- show sdm prefer, 1315 ページ
- show tech-support wireless, 1316 ページ
- show wireless band-select, 1318 ページ
- show wireless client calls, 1319 ページ
- show wireless client dot11, 1320 ページ
- show wireless client location-calibration, 1321 ページ
- show wireless client probing, 1321 ページ
- show wireless client summary, 1322 ページ
- show wireless client timers, 1323 ページ
- show wireless client voice diagnostics, 1323 ページ
- show wireless country, 1324 ページ
- show wireless detail, 1327 ページ
- show wireless dtls connections, 1328 ページ
- show wireless flow-control, 1329 ページ
- show wireless flow-control statistics, 1330 ページ
- show wireless load-balancing, 1331 ページ
- show wireless performance, 1331 ページ
- show wireless pmk-cache, 1332 ページ
- show wireless probe, 1333 ページ

- show wireless sip preferred-call-no, 1334 ページ
- show wireless summary, 1335 ページ
- shutdown, 1336 ページ
- system env temperature threshold yellow, 1336 ページ
- test cable-diagnostics tdr, 1338 ページ
- traceroute mac, 1339 ページ
- traceroute mac ip, 1342 ページ
- trapflags, 1344 ページ
- trapflags client, 1345 ページ
- type, 1346 ページ
- unset, 1347 ページ
- version, 1349 ページ
- wireless client, 1349 ページ
- wireless client mac-address deauthenticate, 1351 ページ
- wireless client mac-address, 1352 ページ
- wireless load-balancing, 1357 ページ
- wireless sip preferred-call-no, 1358 ページ

ap hyperlocation

ハイパーロケーションおよび関連パラメータを設定するには、**ap hyperlocation** コマンドを使用します。ハイパーロケーションおよび関連パラメータを無効にするには、このコマンドの **no** 形式を使用します。

ap hyperlocation [**ble-beacon** {*beacon-id* | **interval***interval-value*} | **threshold** {**detection***value-in-dBm* | **reset***value-btwn-0-99* | **trigger***value-btwn-1-100*}]

[no] ap hyperlocation [**ble-beacon** {*beacon-id* | **interval***interval-value*}|**threshold** {**detection***value-in-dBm* | **reset***value-btwn-0-99* | **trigger***value-btwn-1-100*}]

構文の説明

ble-beacon	BLE ビーコンのパラメータを有効にします。
beacon-id	BLE ビーコン ID。指定できる範囲は 1 ～ 4 です。
interval	BLE ビーコンの間隔を設定します。

interval-value	BLE ビーコンの間隔の値（ヘルツ単位）。値の範囲は 1 ～ 10 です。デフォルトは 1 です。
threshold detection*value-in-dBm*	低い RSSI を持つパケットを除外するためのしきい値を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
threshold reset*value-btwn-0-99*	トリガー後のスキャン サイクルの値をリセットします。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
threshold trigger*value-btwn-1-100*	BAR をクライアントに送信する前のスキャン サイクルの数を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。 （注） ハイパーロケーションしきい値のリセット値がしきい値のトリガー値より小さいことを確認してください。

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが変更されました。**ble-beacon** キーワードが追加されました。

関連トピック

show ap hyperlocation, （1291 ページ）

ap name hyperlocation

アクセス ポイント（AP）のハイパーロケーションおよび関連パラメータを設定するには、**ap name hyperlocation** コマンドを使用します。ハイパーロケーションおよび関連パラメータを無効にするには、このコマンドの no 形式を使用します。

ap name*ap-name***hyperlocationble-beacon***beacon-id*{**major***major-value* | **minor***minor-value* | **txpwr***att-value* }

構文の説明

ap-name	アクセス ポイント名。
ble-beacon	BLE ビーコンのパラメータを設定します。

beacon-id	BLE ビーコン ID。
major	BLE ビーコンの major パラメータを設定します。
major-value	BLE ビーコンの major 値。範囲は 0 ～ 65535 です。デフォルトは 0 です。
minor	BLE ビーコンの minor パラメータを設定します。
minor-value	BLE ビーコンの minor 値。範囲は 0 ～ 65535 です。デフォルトは 0 です。
txpwr	BLE ビーコン減衰レベルを設定します。
att-value	BLE ビーコン減衰値（dBm 単位）。範囲は 0 ～ 52 です。デフォルトは 0 です。

コマンド デフォルト

BLE ビーコンの詳細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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

次に、AP のハイパーロケーションおよび関連パラメータを設定する例を示します。

```
Controller# ap name test-ap hyperlocation ble-beacon 3 txpwr 50
```

hyperlocation

AP グループのハイパーロケーションと関連するパラメータを設定するには、WLAN AP グループコンフィギュレーション（Device(config-apgroup)#）モードで **hyperlocation** コマンドを使用します。AP グループのハイパーロケーションと関連するパラメータを無効にするには、このコマンドの **no** 形式を使用します。

構文の説明

[no] hyperlocation	AP グループのハイパーロケーションを有効または無効にします。
[no] hyperlocation [threshold {detection *value-in-dBm* | **reset** *value-btwn-0-99* | **trigger** *value-btwn-1-100*}]	

threshold detection*value-in-dBm*	パケットをフィルタするためのしきい値を低いRSSIに設定します。コマンドの **[no]** 形式は、しきい値をデフォルト値にリセットします。
threshold reset*value-btwn-0-99*	トリガー後にスキャンサイクルの値をリセットします。コマンドの **[no]** 形式は、しきい値をデフォルト値にリセットします。
threshold trigger*value-btwn-1-100*	BAR をクライアントに送信する前に、スキャン サイクルの数を設定します。コマンドの **[no]** 形式は、しきい値をデフォルト値にリセットします。 （注） ハイパーロケーションしきい値のリセット値は、必ず、しきい値のトリガー値より小さくします。

コマンド モード

WLAN AP グループ 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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

- 次に、パケットをフィルタするためのしきい値を低い RSSI に設定する例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold detection -100
```

- 次に、トリガー後にスキャン サイクルの値をリセットする例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold reset 8
```

- 次に、BAR をクライアントに送信する前にスキャンサイクルの数を設定する例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold trigger 10
```

ap ntp ip

アクセス ポイントから直接到達可能な NTP サーバの IPv4 アドレスを設定するには、**ap ntp ip** コマンドを使用します。NTP サーバに設定されている IPv4 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。

- ハイパーロケーション機能を使用するには NTP が必要です。NTP が定義されていない場合は、ハイパーロケーションが機能しません。
- NTP サーバは AP VLAN から到達可能である必要があります。
- NTP サーバの IPv4 アドレスが設定されていない場合は、グローバルに設定された NTP サーバの IP アドレスが使用されます。

（注） **show** コマンドを使用すると、効果的に使用される NTP サーバの詳細情報が表示されます。たとえば、NTP サーバのグローバルに設定された IPv4 アドレスが 0.0.0.0 である場合は、**show ap hyperlocation** {**summary** | **detail**} コマンドにより、グローバルに設定された NTPサーバの詳細情報が表示されます。

[no] ap ntp ip *ipv4-addr*

構文の説明

ipv4-addr	NTP サーバの IPv4 アドレス。このコマンドの **[no]** 形式を使用すると、NTP 値が 0.0.0.0 にリセットされます。

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

関連トピック

show ap hyperlocation, （1291 ページ）

ntp ip

AP グループの AP によって直接到達可能な NTP サーバの IPv4 アドレスを設定するには、WLAN AP グループ コンフィギュレーション（`Device(config-apgroup)#`）モードで **ntp ip** コマンドを使用します。NTP サーバに設定された IPv4 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。

- NTP は、ハイパーロケーションを動作させるために必須です。NTP が定義されていない場合、ハイパーロケーションは動作しません。
- NTP サーバは、AP VLAN から到達可能である必要があります。
- NTP サーバの IPv4 アドレスが設定されていない場合、グローバルに設定された NTP サーバの IP アドレスが使用されます。

（注） **show** コマンドは効果的に使用されている NTP サーバの詳細を表示します。たとえば、AP NTP サーバ（**ntp ip***ip-addr* コマンドで設定される）が 0.0.0.0 に設定されている場合、**show ap group hyperlocation** {**summary** | **detail**} コマンドは、システム全体の IOS NTP 設定からの NTP サーバのいずれかの詳細を示します。

[no] ntp ip *ipv4-addr*

構文の説明

ipv4-addr	NTP サーバの IPv4 アドレス。このコマンドの **[no]** 形式を使用すると、NTP 値が 0.0.0.0 にリセットされます。

コマンド モード

WLAN AP グループ 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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

arp

Address Resolution Protocol（ARP）テーブルの内容を表示するには、ブート ローダ モードで **arp** コマンドを使用します。

arp [*ip_address*]

構文の説明

ip_address	（任意）ARP テーブルまたは特定の IP アドレスのマッピングを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 テーブルには、IP アドレスと MAC アドレスのマッピングが示されます。

例

次に、ARP テーブルを表示する例を示します。

```
Device: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

関連トピック

セット，（1283 ページ）

boot

実行可能イメージをロードおよびブートして、コマンドライン インターフェイス（CLI）を表示するには、ブート ローダ モードで **boot** コマンドを使用します。

boot [**-post** | **-n** | **-p** | *flag*] *filesystem:/file-url...*

構文の説明

-post	（任意）拡張および総合 POST によってロードされたイメージを実行します。このキーワードを使用すると、POST の完了に要する時間が長くなります。
-n	（任意）起動後すぐに、Cisco IOS デバッガが休止します。
-p	（任意）イメージのロード後すぐに、JTAG デバッガが休止します。
filesystem:	ファイル システムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリ スティックには **usbflash0:** を使用します。
/file-url	ブート可能なイメージのパス（ディレクトリ）および名前。各イメージ名はセミコロンで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

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、デバイスは、BOOT 環境変数が設定されていればその中の情報を使用して、システムを自動的にブートしようとします。

file-url 変数にイメージ名を指定した場合、**boot** コマンドは指定されたイメージをブートしようとします。

ブートローダ **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回のブート処理に使用されることはありません。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

例

次の例では、*new-image.bin* イメージを使用してデバイスをブートする方法を示します。

```
Device: set BOOT flash:/new-images/new-image.bin
Device: boot
```

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。

cat

1 つ以上のファイルの内容を表示するには、ブート ローダ モードで **cat** コマンドを使用します。

cat*filesystem:/file-url...*

構文の説明

filesystem:	ファイル システムを指定します。
/file-url	表示するファイルのパス（ディレクトリ）と名前を指定します。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

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、イメージ ファイルの内容を表示する方法を示します。

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

clear location

特定の無線 ID（RFID）タグまたはデータベース全体のすべての RFID タグ情報をクリアするには、EXEC モードで **clearlocation** コマンドを使用します。

clear location [mac-address *mac-address* | **rfid]**

構文の説明

mac-address*mac-address*	特定の RFID タグの MAC アドレス。
rfid	データベース上のすべての RFID タグを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、データベースからすべての RFID タグ情報をクリアする例を示します。

```
Device> clear location rfid
```

clear location statistics

無線 ID（RFID）統計情報をクリアするには、EXEC モードで **clearlocationstatistics** コマンドを使用します。

clear location 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

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**clear location rfid** コマンドの出力例と、RFID 統計情報をクリアする例を示します。

```
Device> clear location statistics
```

clear nmsp statistics

Network Mobility Services Protocol（NMSP）統計情報をクリアするには、EXEC モードで **clearnmspstatistics** コマンドを使用します。

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

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次は **clear nmsp statistics** コマンドのサンプル出力です。コントローラと接続中の Cisco モビリティ サービス エンジン（MSE）の間で交換される NMSP 情報に関するすべての統計情報をクリアする方法を示します。

```
Device> clear nmsp statistics
```

clear wireless ccx statistics

CCX 統計情報をクリアするには、EXEC モードで **clearwirelessccxstatistics** コマンドを使用します。

clear wireless ccx 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

デフォルトの動作や値はありません。

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**clear wireless ccx statistics** コマンドの出力例と、CCX クライアントに関して収集されたすべての統計情報をクリアする例を示します。

```
Device> clear wireless ccx statistics
```

clear wireless client tsm dot11

特定のアクセスポイント、またはこのクライアントが関連付けられているすべてのアクセスポイントのトラフィック ストリーム メトリック（TSM）統計情報をクリアするには、EXEC モードで **clearwirelessclienttsmdot11** コマンドを使用します。

clear wireless client tsm dot11 {**24ghz| 5ghz**} *client-mac-addr* {**all**| **name** *ap-name*}

構文の説明

24ghz	802.11a ネットワークを指定します。
5ghz	802.11b ネットワークを指定します。
client-mac-addr	クライアントの MAC アドレス。
all	すべてのアクセス ポイントを指定します。
name*ap-name*	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**clear wireless client tsm dot11** コマンドの出力例と、このクライアントが認識されているすべての 5-GHz 無線アクセス ポイント上の MAC アドレス 00:40:96:a8:f7:98 の TSM をクリアする例を示します。

```
Device> clear wireless client tsm dot11 5ghz 00:40:96:a8:f7:98 all
```

clear wireless location s69 statistics

CCXv5 クライアントとの S69 交換に関する統計情報をクリアするには、EXEC モードで **clearwirelesslocations69statistics** コマンドを使用します。

clear wireless location s69 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

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

S69 メッセージは、CCXv5 クライアントと無線インフラストラクチャとの間で交換されます。CCXv5 クライアントは S69 メッセージを使用してロケーション情報を要求します。これに対し、無線インフラストラクチャから S69 応答メッセージが返されます。

例

次に、**clear wireless location s69 statistics** コマンドの出力例と、CCXv5 クライアントとの S69 交換に関する統計情報をクリアする例を示します。

```
Device> clear wireless location s69 statistics
```

copy

ファイルをコピー元からコピー先にコピーするには、ブート ローダ モードで **copy** コマンドを使用します。

copy*filesystem:/source-file-urlfilesystem:/destination-file-url*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/source-file-url	コピー元のパス（ディレクトリ）およびファイル名です。
/destination-file-url	コピー先のパス（ディレクトリ）およびファイル名です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

スラッシュ（/）間に指定できるディレクトリ名は最大 127 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 127 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。

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0: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。

config-ble

BLE ビーコン値を設定するには、config-ble コマンドを使用します。

config-ble { **default**{**enable** | **txpwr**| **uuid** } | **enable**| **exit**| **no**{**enable** | **txpwr**| **uuid***uuid-name* } | **txpwr***att-value*| **uuid**}

構文の説明

default	コマンドをデフォルト値に設定します。
enable	BLE ビーコンを有効にします。
txpwr	BLE ビーコン減衰レベルを設定します。
uuid	汎用一意識別子（UUID）を設定します。
uuid-string	UUID の 16 進数文字列。RFC 標準（RFC4122）で定義されているように、GUI は大文字と小文字の両方のユーザ入力を受け入れますが、入力は小文字で保存されます。
exit	config-ble サブモードを終了します。
no	コマンドを無効にするか、またはデフォルト値を設定します。
att-value	BLE ビーコン減衰値（dBm 単位）。範囲は 0 ～ 52 です。デフォルトは 0 です。

コマンド デフォルト

BLE ビーコン値は設定されていません。

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

BLE ビーコン パラメータを設定するには、このコマンドを使用します。

例

次に、BLE ビーコンを有効にする例を示します。

```
Controller(config-ble)# enable
```

copy startup-config tftp:

スイッチから TFTP サーバに設定をコピーするには、特権 EXEC モードで **copy startup-config tftp:** コマンドを使用します。

copy startup-config tftp:*remote host {ip-address}/{name}*

構文の説明

remote host {ip-address}/{name}	リモート ホストのホスト名または IP アドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

使用上のガイドライン

スイッチから現在の設定をコピーするには、**copy startup-config tftp:** コマンドを実行し、続く指示に従います。設定が TFTP サーバにコピーされます。

次に、別のスイッチへログインし、**copy tftp: startup-config** コマンドを実行して、続く指示に従います。これで、設定は別のスイッチにコピーされます。

例

次に、TFTP サーバに設定をコピーする例を示します。

```
Device: copy startup-config tftp:
Address or name of remote host []?
```

copy tftp: startup-config

TFTP サーバから新しいスイッチに設定をコピーするには、新しいスイッチ上で、特権 EXEC モードで **copy tftp: startup-config** コマンドを使用します。

copy tftp: startup-config*remote host {ip-address}/{name}*

構文の説明

remote host {ip-address}/{name}	リモート ホストのホスト名または IP アドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

使用上のガイドライン

設定をコピーした後、その設定を保存するには、**write memory** コマンドを使用し、その後スイッチをリロードするか、または **copy startup-config running-config** コマンドを実行します。

例

次に、TFTP サーバからスイッチに設定をコピーする例を示します。

```
Device: copy tftp: startup-config
Address or name of remote host []?
```

debug call-admission wireless all

ワイヤレス コール アドミッション制御（CAC）機能のデバッグを有効にするには、特権 EXEC モードで **debugcall-admissionwirelessall** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug call-admission wireless all [**switch** *switch*]

no debug call-admission wireless all [**switch** *switch*]

構文の説明

switch	特定のスイッチに関連付けられるすべてのワイヤレス CAC メッセージのデバッグ オプションを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**debug call-admission wireless switch** コマンドの出力例と、CAC メッセージのデバッグ オプションを有効にする例を示します。

```
Device# debug call-admission wireless switch 1 all
```

debug rfid

無線 ID（RFID）デバッグを設定するには、特権 EXEC モードで **debugrfid** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug rfid {*debug_leaf_name*| **all** | **detail** |**error**|**nmsp**|**receive**}[**filter**|**switch** *switch*]

no debug rfid {*debug_leaf_name*| **all** | **detail** | **error** | **nmsp** | **receive**}[**filter** | **switch** *switch*]

構文の説明

debug_leaf_name	デバッグ リーフ名です。
all	すべての RFID のデバッグを設定します。
detail	RFID 詳細のデバッグを設定します。
error	RFID エラー メッセージのデバッグを設定します。
nmsp	RFID の Network Mobility Services Protocol（NMSP）メッセージのデバッグを設定します。
receive	入力 RFID タグ メッセージのデバッグを設定します。
filter	デバッグ フラグ フィルタ名です。
switch *switch*	デバイスの RFID デバッグを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**debug rfid** コマンドの出力例と、RFID エラー メッセージのデバッグを有効にする例を示します。

```
Device# debug rfid error switch 1
```

debug voice diagnostics mac-address

音声クライアントの音声診断のデバッグを有効にするには、特権 EXEC モードで **debugvoicediagnosticsmac-address** コマンドを使用します。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 voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**

nodebug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**

構文の説明

voice diagnostics	音声クライアントの音声のデバッグを設定します。
mac-address*mac-address1***mac-address***mac-address2*	音声クライアントの MAC アドレスを指定します。
verbose	音声診断の冗長モードを有効にします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

以下は、**debug voice diagnostics mac-address** コマンドの出力例で、MAC アドレスが 00:1f:ca:cf:b6:60 である音声クライアントの音声診断のデバッグを有効にする手順を示しています。

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

debug wps mfp

WPS MFP デバッグ オプションを有効にするには、特権 EXEC モードで **debugwps mfp** コマンドを使用します。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。

構文の説明

wps mfp **debug wps mfp** {**all** | **capwap**| **client** | **detail**| **mm**| **report**}[**switch** *switch*]	WPS MFP デバッグ オプションを設定します。

all	すべての WPS MFP デバッグ メッセージを表示します。
capwap	MFP メッセージを表示します。
client	クライアント MFP メッセージを表示します。
detail	詳細な MFP CAPWAP メッセージを表示します。
mm	MFP モビリティ（コントローラ間）メッセージを表示します。
report	MFP レポートを表示します。
switch *switch*	デバイスの WPS MFP デバッグを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、クライアントの WPS MFP デバッグ オプションを有効にする例を示します。

```
Device# debug wps mfp client switch 1
```

delete

指定されたファイル システムから 1 つ以上のファイルを削除するには、ブート ローダ モードで **delete** コマンドを使用します。

delete*filesystem:/file-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

/file-url...	削除するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

各ファイルを削除する前に確認を求めるプロンプトが デバイス によって表示されます。

例

次の例では、2 つのファイルを削除します。

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

ファイルが削除されたことを確認するには、**dir usbflash0:** ブート ローダ コマンドを入力します。

dir

指定されたファイル システムのファイルおよびディレクトリのリストを表示するには、ブート ローダ モードで **dir** コマンドを使用します。

dir*filesystem:/file-url*

構文の説明

filesystem:	ファイル システムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリ スティックには **usbflash0:** を使用します。

/file-url	（任意）表示するコンテンツが格納されているパス（ディレクトリ）およびディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブート ローダ

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

```
Device: dir flash:
Directory of flash:/
    2  -rwx         561   Mar 01 2013 00:48:15  express_setup.debug
    3  -rwx     2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
    4  -rwx        1048   Mar 01 2013 00:01:39  multiple-fs
    6  drwx         512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
  645 drwx         512   Mar 01 2013 00:01:11  dc_profile_dir
  647 -rwx        4316   Mar 01 2013 01:14:05  config.text
  648 -rwx           5   Mar 01 2013 00:01:39  private-config.text

  96453632 bytes available (25732096 bytes used)
```

表 *47* : *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

フィールド	説明
-rwx	ファイルのアクセス権（次のいずれか、またはすべて） • d：ディレクトリ • r：読み取り可能 • w：書き込み可能 • x：実行可能
1644045	ファイルのサイズ
<date>	最終変更日
env_vars	ファイル名。

関連トピック

mkdir, （1275 ページ）
rmdir, （1281 ページ）

emergency-install

システムで緊急インストールを実行するには、ブート ローダ モードで **emergency-install** コマンドを使用します。

emergency-install*url://<url>*

構文の説明

<url>	緊急インストール バンドル イメージが格納されているファイルの URL と名前です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

インストール操作時にブート フラッシュが消去されます。

例

次に、イメージ ファイルの内容を使用して緊急インストール操作を実行する例を示します。

```
Device: emergency-install tftp:<url>
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
Reading full image into memory.....................done
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042d5c8
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60745294
Initramfs Size    : 0xdc6774/14444404
Compression Format: .mzip

Bootable image at @ ram:0x6042d5c8
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range          \
[0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle                                      \
tftp:<url>


Downloading bundle tftp:<url>...

Validating bundle tftp:<url>...
Installing bundle tftp:<url>...
Verifying bundle tftp:<url>...
Package cat3k_caa-base.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.10.0.100.0.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.\ufffd


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM                     \
+++@@@@@####...++@@++@@++@@++@@++@@++@@++@@done.
Memory Test Pass!
```

```
Base ethernet MAC Address: 20:37:06:ce:25:80
Initializing Flash...

flashfs[7]: 0 files, 1 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 6784000
flashfs[7]: Bytes used: 1024
flashfs[7]: Bytes available: 6782976
flashfs[7]: flashfs fsck took 1 seconds....done Initializing Flash.

The system is not configured to boot automatically. The
following command will finish loading the operating system
software:

    boot
```

exit

以前のモードに戻るか、CLI EXEC モードを終了するには、**exit** コマンドを使用します。

exit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、コンフィギュレーション モードを終了する例を示します。

```
Device(config)# exit
Device#
```

flash_init

flash: ファイル システムを再初期化するには、ブートローダ モードで **flash_init** 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。

コマンド デフォルト

flash: 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	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

flash: ファイル システムは、通常のブート プロセス中に自動的に初期化されます。

このコマンドは、flash: 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。

help

利用可能なコマンドを表示するには、ブート ローダ モードで **help** コマンドを使用します。

help

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

例

次に、利用可能なブート ローダ コマンドのリストを表示する例を示します。

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

license right-to-use

デバイスに使用権アクセス ポイント追加ライセンスを設定するには、特権 EXEC モードで **licenseright-to-use** コマンドを使用します。

license right-to-use {**activate**| **deactivate**} **apcount** |**ipbase** |**ipservices** |**lanbase**

構文の説明

activate	永久または評価 ap-count ライセンスをアクティブ化します。
deactivate	永久または評価 ap-count ライセンスを非アクティブ化します。
apcount*count*	追加する ap-count ライセンスの数を指定します。 設定できる追加ライセンス数は、5 ~ 50 です。
ipbase*count*	スイッチの ipbase ライセンスをアクティブ化します。

ipservices*count*	スイッチの ipservices ライセンスをアクティブ化します。
lanbase*count*	スイッチの lanbase ライセンスをアクティブ化します。

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

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ap-count 評価ライセンスをアクティブ化する例を示します。

```
Device# license right-to-use activate apcount evaluation
Device# end
```

次に、ap-count 永久ライセンスをアクティブ化する例を示します。

```
Device# license right-to-use deactivate apcount evaluation
Device# end
```

次に、新規 ap-count ライセンスを追加する例を示します。

```
Device# license right-to-use activate apcount 500 slot 1
Device# end
```

location

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には、このコマンドの **no** 形式を使用します。

location {**admin-tag** *string*| **algorithm**| **civic-location identifier** {**host**| *id*}| **civic-location identifier** {**host**| *id*}| **elin-location** {*string* |**identifier** *id*}|
expiry{**calibrating-client***timeout-value*|**client***timeout-value*|**rouge-aps***timeout-value*|**tags***timeout-value*}|
geo-location identifier {**host**| *id*}| **notify-threshold**{**client***db*|**rouge-aps***db*|**tags***db*| **plm**{**calibrating**| {**multiband | uniband**}| **client***burst-interval*}| **prefer**{**cdp weight***priority-value*|**lldp-med weight***priority-value*|**static config weight***priority-value*}|**rfid**{**status**
|**timeout***rfid-timeout-value*|**vendor-name***name*}|**rssi-half-life** {
calibrating-client*seconds*|**client***seconds*|**rogue-aps***seconds*|**tags***seconds*}

no location {**admin-tag** *string*| **algorithm**| **civic-location identifier** {**host**| *id*}| **civic-location identifier** {**host**| *id*}| **elin-location** {*string* |**identifier** *id*}|
expiry{**calibrating-client***timeout-value*|**client***timeout-value*|**rouge-aps***timeout-value*|**tags***timeout-value*}|
geo-location identifier {**host**| *id*}| **notify-threshold**{**client***db*|**rouge-aps***db*|**tags***db*| **plm**{**calibrating**| {**multiband | uniband**}| **client***burst-interval*}| **prefer**{**cdp weight***priority-value*|**lldp-med weight***priority-value*|**static config weight***priority-value*}|**rfid**{**status**
|**timeout***rfid-timeout-value*|**vendor-name***name*}|**rssi-half-life** {
calibrating-client*seconds*|**client***seconds*|**rogue-aps***seconds*|**tags***seconds*}

構文の説明

admin-tag*string*	管理タグまたはサイト情報を設定します。英数字形式のサイト情報またはロケーション情報。
algorithm	平均RSSIおよびSNR値に使用されるアルゴリズムを設定します。
civic-location	都市ロケーション情報を設定します。
identifier	都市ロケーション、緊急ロケーション、地理的な場所の名前を指定します。
host	ホストの都市ロケーションや地理空間的な場所を定義します。

id	都市ロケーション、緊急ロケーション、地理的な場所の名前。 （注） LLDP-MED スイッチ 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。
elin-location	緊急ロケーション情報 (ELIN) を設定します。
expiry {calibrating-client | client | rogue-aps | tags} *timeout-value*	調整クライアント、クライアント、不正アクセスポイント、および RFID タグの RSSI タイムアウト値を設定します。 調整クライアントに有効なタイムアウト パラメータ値の範囲は 1 ～ 3600 秒です。デフォルト値は 5 秒です。 クライアント、不正アクセス ポイント、RFID タグに有効なタイムアウト パラメータ値の範囲は 5 ～ 3600 秒です。デフォルト値は 5 秒です。
geo-location	地理空間的なロケーション情報を設定します。
notify-threshold {client| rogue-aps| tags} *db*	RSSI 測定の NMSP 通知しきい値を設定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
calibrating {multiband | uniband} | client *seconds*	調整クライアントのパス損失測定（CCX S60）要求およびクライアントのバースト間隔を設定します。 バースト間隔パラメータに有効な値の範囲は 0 ～ 3600 秒です。
prefer	ロケーション情報のソースのプライオリティを設定します。
rfid	ロケーションの RFID タグ トラッキングを設定します。
rssi-half-life	各種デバイスの RSSI 半減期を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	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 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。**location geo-location identifier** グローバル コンフィギュレーション コマンドを入力後、ジオ 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。

都市ロケーション ID は 250 バイトを超えてはなりません。

ホスト ID はホストの都市ロケーションや地理空間的な場所を設定します。ID がホストではない場合、ID はインターフェイスで参照できる地理空間的なテンプレートまたは都市ロケーションだけを定義します。

hostキーワードは、デバイスの場所を定義します。**identifier** と **host**キーワードを使用して設定可能な都市ロケーション オプションは同じです。都市ロケーション コンフィギュレーション モードで次の都市ロケーション オプションを指定できます。

- **additional-code**：追加都市ロケーション コードを設定します。
- **additional-location-information**：追加都市ロケーション情報を設定します。
- **branch-road-name**：ブランチのロード名を設定します。
- **building**：建物の情報を設定します。
- **city**：都市名を設定します。
- **country**：2 文字の ISO 3166 の国コードを設定します。
- **county**：郡名を設定します。
- **default**：コマンドをデフォルト値に設定します。
- **division**：市の地区の名前を設定します。
- **exit**：都市ロケーション コンフィギュレーション モードを終了します。
- **floor**：階数を設定します。
- **landmark**：目印となる建物の情報を設定します。
- **leading-street-dir**：町名番地に付与される方角を設定します。
- **name**：居住者名を設定します。
- **neighborhood**：ネイバーフッド情報を設定します。
- **no**：指定された都市ロケーション データを拒否し、デフォルト値を設定します。

- **number**：町名番地を設定します。
- **post-office-box**：私書箱を設定します。
- **postal-code**：郵便番号を設定します。
- **postal-community-name**：郵便コミュニティ名を設定します。
- **primary-road-name**：主要道路の名前を設定します。
- **road-section**：道路の区間を設定します。
- **room**：部屋の情報を設定します。
- **seat**：座席の情報を設定します。
- **state**：州の名前を設定します。
- **street-group**：町名番地のグループを設定します。
- **street-name-postmodifier**：町名番地の名前のポストモディファイアを設定します。
- **street-name-premodifier**：町名番地の名前のプレモディファイアを設定します。
- **street-number-suffix**：町名番地の番号のサフィックスを設定します。
- **street-suffix**：町名番地のサフィックスを設定します。
- **sub-branch-road-name**：支線からさらに分岐した道路名を設定します。
- **trailing-street-suffix**：後に続く町名番地のサフィクスを設定します。
- **type-of-place**：場所のタイプを設定します。
- **unit**：単位を設定します。

地理的ロケーションコンフィギュレーションモードで次の地理空間的なロケーション情報を指定できます。

- **altitude**：高さの情報を階数、メートル、またはフィート単位で設定します。
- **latitude**：度、分、秒の緯度情報を設定します。範囲は -90 ～ 90 度です。正の値は、赤道より北側の位置を示します。
- **longitude**：度、分、秒の経度の情報を設定します。範囲は -180 ～ 180 度です。正の値は、グリニッジ子午線の東側の位置を示します。
- **resolution**：緯度と経度の分解能を設定します。分解能値を指定しない場合、10 m のデフォルト値が緯度と経度の分解能パラメータに適用されます。緯度と経度の場合、分解能の単位はメートルで測定されます。分解能の値は小数単位でも指定できます。
- **default**：デフォルトの属性によって、地理的位置を設定します。
- **exit**：地理的ロケーション コンフィギュレーション モードを終了します。
- **no**：指定された地理的パラメータを拒否し、デフォルト値を設定します。

ロケーション TLV を無効にするには、**no lldp med-tlv-select location information** インターフェイス 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。

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。

```
Device(config)# location civic-location identifier 1
Device(config-civic)# number 3550
Device(config-civic)# primary-road-name "Cisco Way"
Device(config-civic)# city "San Jose"
Device(config-civic)# state CA
Device(config-civic)# building 19
Device(config-civic)# room C6
Device(config-civic)# county "Santa Clara"
Device(config-civic)# country US
Device(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。

```
Device(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。

次に、スイッチに、地理空間ロケーション情報を設定する例を示します。

```
Device(config)# location geo-location identifier host
Device(config-geo)# latitude 12.34
Device(config-geo)# longitude 37.23
Device(config-geo)# altitude 5 floor
Device(config-geo)# resolution 12.34
```

設定された地理空間的な場所の詳細を表示するには、**show location geo-location identifier** コマンドを使用します。

location algorithm

RSSI と SNR 値を平均するために使用するアルゴリズムを設定するには、グローバル コンフィギュレーション モードで **locationalgorithm** コマンドを使用します。RSSI と SNR 値を平均するために使用するアルゴリズムを削除するには、このコマンドの **no** 形式を使用します。

location algorithm {**rssi-average | simple**}

no location algorithm {**rssi-average | simple**}

構文の説明

rssi-average	より正確なアルゴリズムが指定されますが、CPU オーバーヘッドが増えます。
simple	CPU オーバーヘッドの少ない、より高速のアルゴリズムが指定されますが、精度が低くなります。

コマンド デフォルト

RSSI-average

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、精度が高い一方、CPU オーバーヘッドが大きいアルゴリズムを設定する例を示します。

```
Device# configure terminal
Device(config)# location algorithm rssi-average
Device(config)# end
```

location expiry

RSSI値の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**locationexpiry**コマンドを使用します。

location expiry {**calibrating-client | client | rogue-aps | tags** } *timeout-value*

構文の説明

calibrating-client	調整クライアントの RSSI タイムアウト値を指定します。
client	（任意）クライアントの RSSI タイムアウト値を指定します。
rogue-aps	不正アクセス ポイントの RSSI タイムアウト値を指定します。
tags	RFID タグの RSSI タイムアウト値を指定します。
timeout-value	調整クライアントに有効なタイムアウト パラメータ値の範囲は 1 ～ 3600 秒です。デフォルト値は 5 秒です。 クライアント、不正アクセス ポイント、RFID タグに有効なタイムアウト パラメータ値の範囲は 5 ～ 3600 秒です。デフォルト値は 5 秒です。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ワイヤレス クライアントの RSSI タイムアウト値を設定する例を示します。

```
Device# configure terminal
Device(config)# location expiry client 1000
Device(config)# end
```

location notify-threshold

RSSI 測定の NMSP 通知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 **locationnotify-threshold** コマンドを使用します。RSSI 測定の NMSP 通知しきい値を削除するには、このコマンドの **no** 形式を使用します。

location notify-threshold {**client | rogue-aps | tags** }*db*

no location notify-threshold {**client | rogue-aps | tags** }

構文の説明

client	クライアントおよび不正クライアントの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
rogue-aps	不正アクセス ポイントの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
tags	RFID タグの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
db	しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。

コマンド デフォルト

グローバルの動作や値はありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、クライアントの NMSP 通知しきい値を 10 dB に設定する例を示します。クライアント RSSI が差分 10 dB で変更されると同時に、通知 NMSP メッセージが MSE に送信されます。

```
Device# configure terminal
Device(config)# location notify-threshold client 10
Device(config)# end
```

location plm calibrating

調整クライアントのパス損失測定（CCX S60）要求を設定するには、グローバル コンフィギュレーション モードで **locationplmcalibrating** コマンドを使用します。

location plm calibrating {**multiband | uniband**}

構文の説明

multiband	関連付けられた 802.11a または 802.11b/g 無線での調整クライアントのパス損失測定要求を指定します。
uniband	関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

単一の無線クライアントには、（無線がデュアルバンドで、2.4 GHz と 5 GHz の両方の帯域でも動作できるとしても）uniband が役立ちます。複数の無線クライアントには、multiband が役立ちます。

次に、関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を設定する例を示します。

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
```

location rfid

ロケーションの RFID タグ トラッキングを設定するには、グローバル コンフィギュレーション モードで **locationrfid** コマンドを使用します。ロケーションの RFID タグ トラッキングを削除するには、このコマンドの **no** 形式を使用します。

location rfid { **status**| **timeout** *seconds*| **vendor-name** *name*}

no location rfid { **status**| **timeout** *seconds*| **vendor-name**}

構文の説明

status	RFID タグのロケーション トラッキングを有効にします。 **no location rfid status** コマンドはタグのロケーション トラッキングを無効にします。
timeout*seconds*	ロケーション RFID タイムアウト値を指定します。 この値は、検出された RFID ロケーション情報が有効と見なされる期間を決定します。設定された期間中にRSSIが変更されても（RSSI しきい値未満）、新しいロケーションは計算されず、メッセージが MSE に送信されます。 有効なタイムアウトの範囲は、60 ～ 7200 秒です。
vendor-name*name*	RFID タグ ベンダー名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

no location rfid status コマンドは、ロケーション RFID ステータスを無効にします。**no location rfid timeout** コマンドは、デフォルトのタイムアウト値に戻します。**no location rfid vendor-name** は、特定のベンダーのトラッキングを無効にします。

次に、スタティック RFID タグのデータ タイムアウトを設定する例を示します。

```
Device# configure terminal
Device(config)# location rfid timeout 1000
Device(config)# end
```

location rssi-half-life

さまざまなデバイスの RSSI 半減期を設定するには、グローバル コンフィギュレーション モードで **locationrssi-half-life** コマンドを使用します。さまざまなデバイスの RSSI 半減期を削除するには、このコマンドの **no** 形式を使用します。

location rssi-half-life {**calibrating-client | client | rogue-aps | tags** }*seconds*

no location rssi-half-life {**calibrating-client | client | rogue-aps | tags** }

構文の説明

calibrating-client	調整クライアントの RSSI 半減期を指定します。
client	クライアントの RSSI 半減期を指定します。
rogue-aps	不正アクセス ポイントの RSSI 半減期を指定します。
tags	RFID タグの RSSI 半減期を指定します。
seconds	半減期パラメータに有効な値は、0、1、2、5、10、20、30、60、90、120、180、または 300 秒です。デフォルト値は 0 秒です。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、クライアントの RSSI 半減期値を 100 秒に設定する例を示します。

```
Device# configure terminal
Device(config)# location rssi-half-life client 100
Device(config)# end
```

mac address-table move update

MAC アドレス テーブル移行更新機能を有効にするには、スイッチ スタックまたはスタンドアロン スイッチのグローバル 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

receive	スイッチが MAC アドレス テーブル移行更新メッセージを処理するように指定します。
transmit	プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、スイッチが MAC アドレス テーブル移行更新メッセージをネットワークの他のスイッチに送信するように指定します。

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
Cisco IOS XE 3.2SE	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提供できます。

プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、アクセス スイッチが MAC アドレステーブル移行更新メッセージを送信するように設定できます。アップリンク スイッチが、MAC アドレステーブル移行更新メッセージを受信および処理するように設定できます。

例

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Device# configure terminal
Device(config)# mac address-table move update transmit
Device(config)# 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。

```
Device# configure terminal
Device(config)# mac address-table move update receive
Device(config)# end
```

設定を確認するには、**show mac address-table move update** 特権 EXEC コマンドを入力します。

mgmt_init

イーサネット管理ポートを再初期化するには、ブートローダ モードで **mgmt_init** コマンドを使用します。

mgmt_init

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

イーサネット管理ポートのデバッグ中にのみ、**mgmt_init** コマンドを使用します。

例

次の例では、イーサネット管理ポートを初期化する方法を示します。

```
Device: mgmt_init
```

mkdir

指定されたファイル システムに 1 つ以上のディレクトリを作成するには、ブート ローダ モードで **mkdir** コマンドを使用します。

mkdir*filesystem:/directory-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/directory-url...	作成するディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 127 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。

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

関連トピック

dir, （1255 ページ）

rmdir, （1281 ページ）

more

1 つ以上のファイルの内容を表示するには、ブート ローダ モードで **more** コマンドを使用します。

more*filesystem:/file-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url...	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

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

次に、ファイルの内容を表示する例を示します。

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

nmsp notification interval

コントローラの Network Mobility Services Protocol（NMSP）通知間隔値をネットワークの遅延に対応するように変更するには、グローバル コンフィギュレーション モードで **nmspnotificationinterval** コマンドを使用します。

nmsp notification interval { **attachment** | **location** | **rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } } }

構文の説明

attachment	アタッチメント情報の集約に使用する時間を指定します。
location	ロケーション情報の集約に使用する時間を指定します。
rssi	RSSI 情報の集約に使用する時間を指定します。
clients	クライアントの時間間隔を指定します。

rfid	RFID タグの時間間隔を指定します。
rogues	不正 AP および不正クライアントの時間間隔を指定します。
ap	不正 AP の集約に使用する時間を指定します。
client	不正なクライアントの集約に使用する時間を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、アクティブな RFID タグの NMSP 通知間隔を 25 秒に設定する例を示します。

```
Device# configure terminal
Device(config)# nmsp notification-interval rfid 25
Device(config)# end
```

次に、デバイスアタッチメント（ネットワークへの接続またはネットワークからの切断）の NMSP 通知間隔を 10 秒に変更する例を示します。

```
Device# configure terminal
Device(config)# nmsp notification-interval attachment 10
Device(config)# end
```

次に、ロケーション パラメータ（ロケーション変更）の NMSP 通知間隔を 20 秒に設定する例を示します。

```
Device# configure terminal
Device(config)# nmsp notification-interval location 20
Device(config)# end
```

no debug all

スイッチのデバッグを無効にするには、特権 EXEC モードで **no debug all** コマンドを使用します。

no debug all

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

例

次に、スイッチでデバッグを無効にする例を示します。

```
Device: no debug all
All possible debugging has been turned off.
```

rename

ファイルの名前を変更するには、ブート コンフィギュレーション モードで **rename** コマンドを使用します。

rename*filesystem:/source-file-urlfilesystem:/destination-file-url*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/source-file-url	元のパス（ディレクトリ）およびファイル名です。
/destination-file-url	新しいパス（ディレクトリ）およびファイル名です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

スラッシュ（/）間に指定できるディレクトリ名は最大 127 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 127 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。

```
Device: rename usbflash0:config.text usbflash0: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。

reset

システムでハード リセットを実行するには、ブート ローダ モードで **reset** コマンドを使用します。ハード リセットを行うと、デバイスの電源切断後に電源を投入する手順と同様に、プロセッサ、レジスタ、およびメモリの内容が消去されます。

reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

例

次の例では、システムをリセットする方法を示します。

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

関連トピック

reset, （1280 ページ）

reset, （1280 ページ）

test cable-diagnostics tdr, （1338 ページ）

rmdir

指定されたファイル システムから 1 つ以上の空のディレクトリを削除するには、ブート ローダ モードで **rmdir** コマンドを使用します。

rmdir*filesystem:/directory-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/directory-url...	削除する空のディレクトリのパス（ディレクトリ）および名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

デバイスは、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を出します。

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。

```
Device: rmdir usbflash0: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。

関連トピック

dir, （1255 ページ）

dir, （1255 ページ）

sdm prefer

スイッチで使用する SDM テンプレートを指定するには、グローバル コンフィギュレーション モードで **sdm prefer** コマンドを使用します。

sdm prefer {**advanced**}

構文の説明

advanced	NetFlow などの高度な機能をサポートします。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デバイス スタックでは、すべてのスタック メンバが、アクティブなデバイスに保存された同一の SDM テンプレートを使用する必要があります。

新規デバイスがスタックに追加されると、アクティブ デバイスに保存された SDM コンフィギュレーションは、個々のデバイスに設定されているテンプレートを上書きします。

例

次に、高度なテンプレートを設定する例を示します。

```
Device(config)# sdm prefer advanced
Device(config)# exit
Device# reload
```

関連トピック

show sdm prefer, （1315 ページ）

セット

環境変数を設定または表示するには、ブート ローダ モードで **set** コマンドを使用します。環境変数は、ブート ローダまたはデバイス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ます。

set *variable value*

構文の説明

variable value	*variable* および *value* の適切な値には、次のいずれかのキーワードを使用します。 **MANUAL_BOOT**：デバイスの起動を自動で行うか手動で行うかどうかを決定します。 有効な値は 1/Yes と 0/No です。0 または No 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ます。他の値に設定されている場合は、ブート ローダ モードから手動でデバイス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を識別します。

BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイルシステムで最初に検出した起動可能なファイルを起動しようとします。

ENABLE_BREAK：ユーザがコンソールの Break キーを押すと自動起動プロセスを中断できるようになります。

有効な値は 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 キーを押すことで、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を識別します。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。

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する文字列を指定します。

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を指定します。

BAUD*rate*：コンソールのボー レートに使用する 1 秒あたりのビット数（b/s）を指定します。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。指定できる範囲は 0 ～ 128000 b/s 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。

SWITCH_NUMBER*stack-member-number*：スタック メンバのメンバ番号を変更します。

SWITCH_PRIORITY*priority-number*：スタック メンバのプライオリティ値を変更します。

コマンド 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 デバイス：

CONFIG_FILE: config.text

BAUD：9600 b/s

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 システムに保管されます。ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。

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“”）が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	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

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 メモリに保管されます。

通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**boot manual** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

BOOT 環境変数は、**boot system***filesystem:/file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ENABLE_BREAK 環境変数は、**boot enable-break** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

HELPER 環境変数は、**boot helper***filesystem:/file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

CONFIG_FILE 環境変数は、**boot config-file flash:***/file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH_NUMBER 環境変数は、**switch***current-stack-member-number***renumber***new-stack-member-number* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH_PRIORITY 環境変数は、デバイス*stack-member-number***priority***priority-number* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ブート ローダのプロンプト ストリング（PS1）には、等号（=）を除く、出力可能な文字列を 120 文字まで指定できます。

例

次に、SWITCH_PRIORITY 環境変数を設定する例を示します。

```
Device: set SWITCH_PRIORITY 2
```

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。

関連トピック

reset, （1280 ページ）

unset, （1347 ページ）

show avc client

上位アプリケーションの数に関する情報を表示するには、特権 EXEC モードで **show avc client** コマンドを使用します。

show avc client *client-mac* **top** *n***application**[**aggregate** | **upstream** | **downstream**]

構文の説明

client*client-mac*	クライアントの MAC アドレスを指定します。
top*n***application**	特定のクライアントの上位「N」個のアプリケーションの数を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show avc client** コマンドの出力例を示します。

```
Device# sh avc client 0040.96ae.65ec top 10 application aggregate

Cumulative Stats:

No.  AppName      Packet-Count    Byte-Count       AvgPkt-Size     usage%
---------------------------------------------------------------------------
1    skinny          7343            449860           61              94
2    unknown         99              13631            137             3
3    dhcp            18              8752             486             2
4    http            18              3264             181             1
5    tftp            9               534              59              0
6    dns             2               224              112             0

Last Interval(90 seconds) Stats:

No.  AppName     Packet-Count     Byte-Count       AvgPkt-Size      usage%
---------------------------------------------------------------------------
1    skinny          9               540              60               100
```

show avc wlan

上位のアプリケーションおよびそれらのアプリケーションを使用しているユーザに関する情報を表示するには、特権 EXEC モードで **show avc wlan** コマンドを使用します。

show avc wlan *ssid* **top** *n* **application**[**aggregate** | **upstream** | **downstream**]

構文の説明

wlan *ssid*	WLAN のサービス セット識別子（SSID）を指定します。
top *n***application**	上位「N」個のアプリケーションの数を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show avc wlan** コマンドの出力例を示します。

```
Device# show avc wlan Lobby_WLAN top 10 application aggregate

Cumulative Stats:

No.  AppName           Packet-Count          Byte-Count          AvgPkt-Size  usage%
---------------------------------------------------------------------------------------
1    ssl               10598677              1979525706          997          42
2    vnc               5550900               3764612847          678          14
3    http              3043131               2691327197          884          10
4    unknown           1856297               1140264956          614          4
5    video-over-http   1625019               2063335150          1269         8
6    binary-over-http  1329115               1744190344          1312         6
7    webex-meeting     1146872               540713787           471          2
8    rtp               923900                635650544           688          2
9    unknown           752341                911000213           1210         3
10   youtube           631085                706636186           1119         3

Last Interval(90 seconds) Stats:

No.  AppName          Packet-Count          Byte-Count            AvgPkt-Size  usage%
-------------------------------------------------------------------------------------
1    vnc              687093                602731844             877          68
2    video-over-http  213272                279831588             1312         31
3    ssl              6515                  5029365               771          1
4    webex-meeting    3649                  1722663               472          0
5    http             2634                  1334355               506          0
6    unknown          1436                  99412                 69           0
7    google-services  722                   378121                523          0
8    linkedin         655                   393263                600          0
9    exchange         432                   167390                387          0
10   gtalk-chat       330                   17330                 52           0
```

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

interface-id	TDR が実行されているインターフェイスを指定します。

コマンド デフォルト

特権EXECの動作や値はありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 は、銅線のイーサネット 10/100/100 ポートだけでサポートされます。10 ギガビット イーサネット ポート、および Small Form-Factor Pluggable（SFP）モジュール ポートではサポートされません。

例

次の例では、デバイス での **show cable-diagnostics tdr interface***interface-id* コマンドの出力を示します。

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/23
  TDR test last run on: March 01 00:04:08
  Interface  Speed  Local pair  Pair length         Remote pair   Pair status
  ---------  -----  ----------  ------------------  -----------  --------------------
  Gi1/0/23   1000M  Pair A      1    +/- 1 meters   Pair A       Normal
                    Pair B      1    +/- 1 meters   Pair B       Normal
                    Pair C      1    +/- 1 meters   Pair C       Normal
                    Pair D      1    +/- 1 meters   Pair D       Normal
```

表 *48*：*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 が実行されているインターフェイス。
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	デバイスに関するケーブルの問題の場所。次のいずれかの場合に限り、TDR は場所を特定できます。 • ケーブルが正しく接続され、リンクがアップ状態で、インターフェイス速度が 1000 Mb/s である場合 • ケーブルが断線している場合 • ケーブルがショートしている場合

フィールド	説明
Remote pair	ローカルペアが接続されたワイヤペア名。ケーブルが正しく接続されリンクがアップ状態である場合だけ、TDR はリモート ペアについて確認します。
Pair status	TDR が実行されているワイヤ ペアのステータス • Normal：ワイヤ ペアが正しく接続されています。 • Not completed：テストは実行中で、完了していません。 • Not supported：インターフェイスは TDR をサポートしません。 • Open：ワイヤ ペアが断線しています。 • Shorted：ワイヤ ペアがショートしています。 • ImpedanceMis：インピーダンスが一致しません。 • Short/Impedance Mismatched：インピーダンスが一致しないかケーブルがショートしています。 • InProgress：診断テストが進行中です。

次の例では、TDR が実行されているときの **show interface***interface-id* コマンドの出力を示します。

```
Device# show interface gigabitethernet1/0/2
  gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が実行されていないときの **show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/2
  % TDR test was never issued on gigabitethernet1/0/2
```

インターフェイスで TDR がサポートされない場合、次のメッセージが表示されます。

```
% TDR test is not supported on デバイス 1
```

関連トピック

test cable-diagnostics tdr, （1338 ページ）

show ap hyperlocation

ハイパーロケーション設定に関するサマリーまたは詳細情報を表示するには、**show ap hyperlocation** コマンドを使用します。

show ap hyperlocation {**ble-beacon**| **summary** | **detail**}

構文の説明

ble-beacon	設定済み BLE ビーコンのリストを表示します。
summary	全体的な設定値と動作値を表示します。
detail	全体的な設定値と動作値、および各 AP に関する詳細情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが変更されました。**ble-beacon** キーワードが追加されました。

使用上のガイドライン

ハイパーロケーションの動作を可能にするには、次の条件を満たす必要があります。

- ハイパーロケーションが有効な Cisco Connected Mobile Experiences（CMX）が 1 つ以上存在している。
- ハイパーロケーション管理状態が動作可能になっている。

- AP Network Time Protocol（NTP）または IOS NTP のいずれかが設定されている。

例

次に、ハイパーロケーション設定のサマリーを表示する例を示します。

```
Device# show ap hyperlocation summary

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

次に、ハイパーロケーション設定に関する詳細情報を表示する例を示します。

```
Device# show ap hyperlocation detail

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8

AP Name                  Radio MAC        Method    Hyperlocation
-----------------------------------------------------------------
AP84b8.0252.b930         84b8.0216.c721   HALO      Enabled
AP84b8.0265.5540         84b8.0243.8796   WSM       Enabled
APf07f.0635.2d40         f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0         f4cf.e223.ba31   HALO      Enabled
```

show ap name hyperlocation

アクセス ポイント（AP）のハイパーロケーション設定の概要または詳細情報を表示するには、**show ap name hyperlocation** コマンドを使用します。

show ap name*ap-name* **hyperlocationble-beacon**

構文の説明

ap-name	アクセス ポイント名。
hyperlocation	AP のハイパーロケーション情報を表示します。
ble-beacon	AP の BLE ビーコン設定を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

次に、AP の BLE ビーコン設定を表示する例を示します。

```
Switch# show ap name test-ap hyperlocation ble-beacon

ID  Major  Minor  TX Power(dBm)
------------------------------
0   0      0      0
1   0      0      0
2   0      0      0
3   0      0      0
```

show ap group *ap-group-name* hyperlocation

AP グループのハイパーロケーション設定のサマリーまたは詳細情報を表示するには、**show ap group***ap-group-name***hyperlocation** コマンドを使用します。

show ap group hyperlocation {**summary** | **detail**}

構文の説明

summary	AP グループの全体的な設定値（AP グループ固有）および動作ステータスとパラメータを表示します。
detail	AP グループの全体的な設定値（AP グループ固有）と AP ごとの設定値の両方および動作ステータスを表示します。リストされている AP は、AP グループに属するもののみです。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、AP グループのハイパーロケーション設定のサマリーを表示する例を示します。

```
Device# show ap group my-ap-group hyperlocation summary

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9
```

（注） ハイパーロケーションの動作を可能にするには、次の条件を満たす必要があります。

- ハイパーロケーションが有効な Cisco CMX が 1 つ以上存在する
- ハイパーロケーション管理状態が動作可能である
- AP NTP または IOS NTP のいずれかが設定されている

次に、AP グループのハイパーロケーション設定に関する詳細情報を表示する例を示します。

```
Device# show ap group my-ap-group hyperlocation detail

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9

Values for APs in all AP Groups:

AP Name                  Radio MAC        Method    Hyperlocation
-----------------------------------------------------------------
APf07f.0635.2d40         f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0         f4cf.e223.ba31   Local     Enabled
```

show debug

スイッチで使用できるすべての debug コマンドを表示するには、特権 EXEC モードで **show debug** コマンドを使用します。

show debug

show debug condition*Condition identifier*| *All conditions*

構文の説明

Condition identifier	使用される条件識別子の値を設定します。範囲は、1 ～ 1000 です。
All conditions	使用可能なすべての条件付きデバッグオプションを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	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。さらに、debugコマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用するのが最良です。このような時間帯を選んでデバッグを実行すると、debugコマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。

例

次に、**show debug** コマンドの出力例を示します。

```
Device# show debug condition all
```

デバッグを無効にするには、**no debug all** コマンドを使用します。

show env

スイッチ（スタンドアロン スイッチ、スタック マスター、またはスタック メンバ）のファン、温度、および電源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** | **fan** | **power**[**all** | **switch** [*switch-number*]] | **stack** [*stack-number*] | **temperature** [**status**] }

構文の説明

all	ファン、温度、および電源環境のステータスを表示します。
fan	スイッチのファンの状態を表示します。
power	電源装置のステータスを表示します。
all	（任意）すべての電源装置のステータスを表示します。
switch*switch-number*	（任意）特定のスイッチの電源装置のステータスを表示します。
stack*switch-number*	（任意）スタックの各スイッチまたは指定されたスイッチのすべての環境ステータスを表示します。指定できる範囲は、スタック内のスイッチ メンバ番号に従って 1 ～ 9 です。
temperature	スイッチの温度ステータスを表示します。
status	（任意）温度ステータスとしきい値を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

任意のメンバ スイッチからスタック内のスイッチに関する情報を表示するには、**show env stack** [*switch-number*] コマンドを使用します。

スイッチの温度ステータスとしきい値レベルを表示するには、**show env temperature status** コマンドを使用します。

例

次の例では、マスター スイッチからスタック メンバ 1 に関する情報を表示する方法を示します。

```
Device> show env stack 1
Device 1:
Device Fan 1 is OK
Device Fan 2 is OK
Device Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
Device 1: SYSTEM TEMPERATURE is OK
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

Device>
```

次に、温度値、状態、およびしきい値を表示する例を示します。

```
Device> show env temperature status
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

Device>
```

表 *49*：*show env temperature status* コマンド出力のステート

ステート	説明
Green	スイッチの温度が正常な動作範囲にあります。
Yellow	温度が警告範囲にあります。スイッチの外の周辺温度を確認する必要があります。
Red	温度がクリティカル範囲にあります。温度がこの範囲にある場合、スイッチが正常に実行されない可能性があります。

show env xps

Cisco eXpandable Power System（XPS）2200 のバジェット配分、設定、電力、およびシステム電源情報を表示するには、特権 EXEC モードで **show env xps** コマンドを使用します。

show env xps { **budgeting** | **configuration** | **port** [**all** | *number*] | **power** | **system** | **thermal** | **upgrade** | **version** }

構文の説明

budgeting	XPS電力バジェットの配分（電源スタックに含まれるすべてのスイッチに対する電力の割り当て量とバジェット量）を表示します。
configuration	power xps 特権 EXEC コマンドを実行した結果の設定を表示します。XPS設定はXPSに保存されます。show env xps configuration コマンドを入力すると、デフォルト以外の設定が取得されます。
port [**all** | *number*]	すべてのポートまたは指定のXPSポートの設定とステータスを表示します。ポート番号は、1～9です。
power	XPS 電源装置のステータスを表示します。
system	XPS システム ステータスを表示します。
thermal	XPS 温度ステータスを表示します。
upgrade	XPS アップグレード ステータスを表示します。
version	XPS バージョンの詳細を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(55)SE1	このコマンドが導入されました。

使用上のガイドライン

XPS 2200 の情報を表示するには、**show env xps** 特権 EXEC コマンドを使用します。

例

次に、show env xps budgeting コマンドの出力例を示します。

```
Switch#
=======
```

```
XPS 0101.0100.0000 :
=========================================================
Data                  Current    Power     Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
----  --------  ----  ----  ---------- ---------  ------ 1     -        -    715  SP-PS
   223
    1543
2     -        -    -    SP-PS      223       223
3     -        -    -    -          -         -
4     -        -    -    -          -         -
5     -        -    -    -          -         -
6     -        -    -    -          -         -
7     -        -    -    -          -         -
8     -        -    -    -          -         -
9     1        1100 -    RPS-NB     223        070
XPS  -        -    1100  -          -
```

次に、show env xps configuration コマンドの出力例を示します。

```
Switch# show env xps configuration
=============================================
XPS 0101.0100.0000 :
=============================================
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4
```

次に、show env xps port all コマンドの出力例を示します。

```
Switch#
XPS 010



----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 1
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 2
----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 2
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 3
----------------------------------------
Port name          : -
Connected          : No
Mode               : Enabled (On)
Priority           : 3
Data stack switch # : - Configured role    : Auto-SP Run mode            : -
Cable faults
<output truncated>
```

次に、show env xps power コマンドの出力例を示します。

```
================================================================================
XPS 0101.0100.0000 :
================================================================================
Port-Supply SW PID                 Serial#     Status          Mode Watts
----------- -- ------------------  ----------- --------------  ----  -----
XPS-A           Not present
XPS-B           NG3K-PWR-1100WAC   LIT13320NTV OK              SP   1100
1-A         -  -                   -           -
1-B         -  -                   -           -               SP    715
```

```
2-A         -  -                    -           -
2-B         -  -                    -           -
9-A                      100WAC    LIT141307RK OK              RPS  1100
9-B                   esent
```

次に、show env xps system コマンドの出力例を示します。

```
Switch#
=======


XPS 0101.0100.0000 :
================================================================================
XPS                        Cfg  Cfg      RPS Switch  Current    Data Port  XPS Port Name

Mode Role    Pri Conn    Role-State  Switch #
----  --------------------  ---- --------  --- ------  ----------  --------
1     -                    On   Auto-SP  1   Yes     SP-PS      -
2     -                    On   Auto-SP  2   Yes     SP-PS      -
3     -                    On   Auto-SP  3   No      -          -
4     none                 On   Auto-SP  5   No      -          -
5     -                    Off  Auto-SP  6   No      -          -
6     -                    On   Auto-SP  7   No      -          -
7     -                    On   Auto-SP  8   No      -          -
8     -                    On   Auto-SP  9   No      -
9     test                 On   Auto-SP  4   Yes     RPS-NB
```

次に、show env xps thermal コマンドの出力例を示します。

```
Switch#
=======


XPS 0101.0100.0000 :
=============================================
Fan  Status
----  ------------
1     OK
2     OK
3     NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK
```

次に、アップグレードが実行されていない場合の show env xps upgrade コマンドの出力例を示します。

```
Switch# show env xps upgrade
No XPS is connected and upgrading.
```

次に、アップグレードが進行中の場合の show env xps upgrade コマンドの出力例を示します。

```
Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
-- ----------- ----
1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 1%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Reloading 100%
Switch#
```

```
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.
```

次に、show env xps version コマンドの出力例を示します。

```
Switch# show env xps version
===============================================
XPS 0022.bdd7.9b14:
===============================================
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18
```

表 *50*：関連コマンド

コマンド	説明
power xps（グローバル コンフィギュレーション コマンド）	XPS と XPS ポートの名前を設定します。
power xps（特権 EXEC コマンド）	XPS ポートとシステムを設定します。

show flow monitor

Flexible NetFlow フロー モニタのステータスと統計情報を表示するには、特権 EXEC モードで **showflowmonitor** コマンドを使用します。

show flow monitor [**broker** [**detail**| **picture**]| [**name**] *monitor-name* [**cache** [**format** {**csv**| **record**| **table**}]]| **provisioning**| **statistics**]

構文の説明

broker	（任意）フロー モニタのブローカの状態に関する情報を表示します。
detail	（任意）フロー モニタのブローカに関する詳細情報を表示します。
picture	（任意）ブローカ状態の画像を表示します。
name	（任意）フロー モニタの名前を指定します。
monitor-name	（任意）事前に設定されたフロー モニタの名前。
cache	（任意）フロー モニタのキャッシュの内容を表示します。
format	（任意）ディスプレイ出力のフォーマット オプションのいずれかを使用することを指定します。
csv	（任意）フローモニタのキャッシュの内容をカンマ区切り値（CSV）形式で表示します。

record	（任意）フロー モニタのキャッシュの内容をレコード形式で表示します。
table	（任意）フロー モニタのキャッシュの内容を表形式で表示します。
provisioning	（任意）フロー モニタのプロビジョニング情報を表示します。
statistics	（任意）フロー モニタの統計情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

cache キーワードでは、デフォルトでレコード形式が使用されます。

showflowmonitor*monitor-name***cache** コマンドのディスプレイ出力に含まれる大文字のフィールド名は、フローを識別するために Flexible NetFlow で使用されるキー フィールドです。
showflowmonitor*monitor-name***cache** コマンドのディスプレイ出力に含まれる小文字のフィールド名は、Flexible NetFlow がキャッシュの追加データとして値を収集する非キー フィールドです。

次の例では、フロー モニタのステータスを表示します。

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *51*：*show flow monitor monitor-name* フィールドの説明

フィールド	説明
Flow Monitor	設定したフロー モニタの名前。
説明	モニタに設定した説明、またはユーザ定義のデフォルトの説明。
Flow Record	フロー モニタに割り当てられたフロー レコード。
Flow Exporter	フローモニタに割り当てられたエクスポータ。
Cache	フロー モニタのキャッシュに関する情報。
Type	フロー モニタのキャッシュ タイプ。この値は常に normal となります。これが唯一サポートされているキャッシュ タイプです。
Status	フロー モニタのキャッシュのステータス。 次の値が可能です。 • allocated：キャッシュが割り当てられています。 • being deleted：キャッシュが削除されています。 • not allocated：キャッシュが割り当てられていません。
Size	現在のキャッシュ サイズ。
Inactive Timeout	非アクティブ タイムアウトの現在の値（秒単位）。
Active Timeout	アクティブ タイムアウトの現在の値（秒単位）。

次の例では、FLOW-MONITOR-1 という名前のフローモニタのステータス、統計情報、およびデータを表示します。

```
Device# show flow monitor FLOW-MONITOR-1 cache
  Cache type:                               Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                               1

  Flows added:                                   3
```

```
  Flows aged:                                 2
    - Active timeout      (   300 secs)       2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001:DB8::1
IPV6 DESTINATION ADDRESS:                2001:DB8:1::1
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *52*：*show flow monitor monitor-name cache* フィールドの説明

フィールド	説明
Cache type	フロー モニタのキャッシュ タイプ。この値は常に normal となります。これが唯一サポートされているキャッシュ タイプです。
Cache Size	キャッシュ内のエントリ数。
Current entries	キャッシュ内の使用中のエントリ数。
Flows added	キャッシュの作成後にキャッシュに追加されたフロー
Flows aged	キャッシュの作成後に期限切れになったフロー
Active timeout	アクティブ タイムアウトの現在の値（秒単位）。
Inactive timeout	非アクティブ タイムアウトの現在の値（秒単位）。
DATALINK MAC SOURCE ADDRESS INPUT	入力パケットの MAC 送信元アドレス。
DATALINK MAC DESTINATION ADDRESS INPUT	入力パケットの MAC 宛先アドレス。
IPV6 SOURCE ADDRESS	IPv6 送信元アドレスです。
IPV6 DESTINATION ADDRESS	IPv6 宛先アドレス。
TRNS SOURCE PORT	トランスポート プロトコルの送信元ポート。

フィールド	説明
TRNS DESTINATION PORT	トランスポート プロトコルの宛先ポート。
IP VERSION	IP バージョン。
IP PROTOCOL	プロトコル番号。
IP TOS	IP タイプ オブ サービス（ToS）の値。
IP TTL	IP 存続可能時間（TTL）の値。
tcp flags	TCP フラグの値。
counter bytes	カウントされたバイト数。
counter packets	カウントされたパケット数。

次の例では、FLOW-MONITOR-1 という名前のフローモニタのステータス、統計情報、およびデータを表形式で表示します。

```
Device# show flow monitor FLOW-MONITOR-1 cache format table
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2

DATALINK MAC SRC ADDR INPUT  DATALINK MAC DST ADDR INPUT  IPV6 SRC ADDR  IPV6 DST ADDR
TRNS SRC PORT  TRNS DST PORT  IP VERSION  IP PROT  IP TOS  IP TTL  tcp flags  bytes long
pkts long
===========================  ===========================  =============  =============
=============  =============  ==========  =======  ======  ======  =========  ==========
=========
0000.0000.1000               6400.F125.59E6               2001:DB8::1    2001:DB8:1::1
       1111           2222           6        6  0x05        11  0x20        132059538
1158417
```

次の例では、FLOW-MONITOR-IPv6 という名前のフロー モニタ（キャッシュに IPv6 データを格納）のステータス、統計情報、およびデータをレコード形式で表示します。

```
Device# show flow monitor name FLOW-MONITOR-IPv6 cache format record
  Cache type:                                 Normal (Platform cache)
  Cache size:                                Unknown
  Current entries:                                 1

  Flows added:                                     3
  Flows aged:                                      2
    - Active timeout      (   300 secs)            2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001::2
IPV6 DESTINATION ADDRESS:                2002::2
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
```

```
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

次の例では、フロー モニタのステータスと統計情報を表示します。

```
Device# show flow monitor FLOW-MONITOR-1 statistics
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2
```

関連トピック

clear flow monitor, （72 ページ）

debug flow monitor, （82 ページ）

show license right-to-use

デバイスにインストールされている apcount adder ライセンスの詳細情報を表示するには、EXEC モードで **show license right-to-use** コマンドを使用します。

show license right-to-use{**default**| **detail**| **eula**| **mismatch**| **slot**| **summary**| **usage**}

構文の説明

default	デフォルトのライセンス情報を表示します。
detail	スタック内のすべてのライセンスの詳細を表示します。
EULA	EULA テキストを表示します。
mismatch	一致しないライセンス情報を表示します。
slot	スイッチ番号を指定します。
summary	スタック全体の統合ライセンス情報を表示します。
usage	すべてのライセンスの使用状況の詳細を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show license right-to-use usage** コマンドの出力例として、すべての詳細情報を表示します。

```
Device# show license right-to-use usage

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
--------------------------------------------------------------------------
 1      ipservices     permanent    0 :0 :1                yes   yes
 1      ipbase         permanent    0 :0 :0                no    no
 1      ipbase         evaluation   0 :0 :0                no    no
 1      lanbase        permanent    0 :0 :7                no    yes
 1      apcount        evaluation   0 :0 :0                no    no
 1      apcount        base         0 :0 :0                no    no
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes

Device#
```

次に、**show license right-to-use detail** コマンドの出力例として、ライセンスの詳細情報を表示します。

```
Device# show license right-to-use detail

Index 1:  License Name: apcount
           Period left: 16
           License Type: evaluation
           License State: Not Activated
           License Count: 1000
           License Location: Slot 1
Index 2:  License Name: apcount
           Period left: Lifetime
           License Type: adder
           License State: Active, In use
           License Count: 125
           License Location: Slot 1
```

次に、評価ライセンスがアクティブな場合の **show license right-to-use summary** コマンドの出力例を示します。

```
Device# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  apcount      evaluation  1000     50

-----------------------------------------------

Evaluation AP-Count: Enabled
Total AP Count Licenses: 1000
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 900
```

次に、adder ライセンスがアクティブな場合の **show license right-to-use summary** コマンドの出力例を示します。

```
Device# show license right-to-use summary
  License Name    Type     Count   Period left
------------------------------------------------
apcount      adder       125      Lifetime

------------------------------------------

Evaluation AP-Count: Disabled
Total AP Count Licenses: 125
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 25
```

show location

ロケーション情報を表示するには、特権 EXEC モードで **show location** コマンドを使用します。

show location {**detail** *mac-addr*| **plm**| **statistics**| **summary rfid**| **rfid** {**client**| **config**| **detail** *MAC-addr*| **summary**}}

構文の説明

detail*mac-addr*	特定のクライアントのRSSIテーブルとともに詳細なロケーション情報を表示します。
plm	ロケーション パス損失測定（CCX S60）の設定を表示します。
statistics	ロケーションベースのシステム統計情報を表示します。
summary	ロケーションベースのシステム概要情報を表示します。
rfid	RFID タグ トラッキング情報を表示します。
client	クライアントである RFID タグの概要を表示します。
config	RFID タグ トラッキングの設定オプションを表示します。
detail*MAC-addr*	1 つの RFID タグの詳細情報を表示します。
summary	既知のすべての RFID タグの概要情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show location plm** コマンドの出力例を示します。

```
Device# show location plm
Location Path Loss Configuration

Calbration client      : Disabled, Radio: Multiband
Normal clients         : Disabled
Burst interval         : 60
```

show location ap-detect

指定されたアクセス ポイントで検出されたロケーション情報を表示するには、特権 EXEC モードで **show location ap-detect** コマンドを使用します。

show location ap-detect {**all| client| rfid| rogue-ap| rogue-client**}*ap-name*

構文の説明

all	クライアント、RFID、不正アクセス ポイント、不正クライアントの情報を表示します。
client	クライアント情報を表示します。
rfid	RFID 情報を表示します。
rogue-ap	不正アクセス ポイントの情報を表示します。
rogue-client	不正クライアントの情報を表示します。
ap-name	特定のアクセス ポイント名。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show location ap-detect client** コマンドの出力例を示します。

```
Device# show location ap-detect client AP02
Clients

MAC Address       Status            Slot  Antenna     RSSI
------------------------------------------------------------
2477.0389.96ac    Associated           1        0      -60
2477.0389.96ac    Associated           1        1      -61
2477.0389.96ac    Associated           0        0      -46
2477.0389.96ac    Associated           0        1      -41


RFID Tags


Rogue AP's


Rogue Clients

MAC Address         State               Slot     Rssi
------------------------------------------------------
0040.96b3.bce6      Alert               1        -58
586d.8ff0.891a      Alert               1        -72
```

show mac address-table move update

デバイス 上の MAC アドレス テーブル移動更新情報を表示するには、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

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

例

次の例では、**show mac address-table move update** コマンドの出力を示します。

```
Device# 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
```

show nmsp

Network Mobility Services Protocol（NMSP）構成の設定を表示するには、**shownmsp** コマンドを使用します。

show nmsp {**attachment**| {**suppress interfaces**}| **capability**| **notification interval**| **statistics** {**connection**| **summary**}| **status**| **subscription detail** [*ip-addr*]| **summary**}

構文の説明

attachmentsuppressinterfaces	アタッチメント抑制インターフェイスを表示します。
capability	NMSP 機能を表示します。
notificationinterval	NMSP 通知間隔を表示します。
statisticsconnection	すべての接続別カウンタを表示します。

statisticssummary	NMSP カウンタを表示します。
status	アクティブな NMSP 接続のステータスを表示します。
subscriptiondetail*ip-addr*	特定の IP アドレスでサブスクライブされている NMSP サービスについてのみ詳細を表示します。
subscriptionsummary	コントローラがサブスクライブされているすべての NMSP サービスの詳細を表示します。特定の IP アドレスでサブスクライブされている NMSP サービスについてのみ詳細を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show nmsp notification interval** コマンドの出力例を示します。

```
Device#  show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
 Client               : 2 sec
 RFID                 : 2 sec
 Rogue AP             : 2 sec
 Rogue Client         : 2 sec
Attachment Interval   : 30 sec
Location Interval     : 30 sec
```

show platform integrity

起動段階のチェックサム レコードを表示するには、特権 EXEC モードで **show platform integrity** コマンドを使用します。

show platform integrity [**sign** [**nonce** <*nonce*>]]

構文の説明

sign	（任意）署名を表示します。
nonce	（任意）ナンス値を入力します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

例

次に、起動段階のチェックサム レコードを表示する例を示します。

```
Device# show platform integrity sign

PCR0: EE47F8644C2887D9BD4DE3E468DD27EB93F4A606006A0B7006E2928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA266848B32924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature:
816C5A29741BBAC1961C109FFC36DA5459A44DBF211025F539AFB4868EF91834C05789
5DAFBC7474F301916B7D0D08ABE5E05E66598426A73E921024C21504383228B6787B74
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEEFD8777AA77F482EC4B
731A09826A41FB3EFFC46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAEE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
Platform: WS-C3650-12X48UZ
```

show platform sudi certificate

特定の SUDI のチェックサム レコードを表示するには、特権 EXEC モードで **show platform sudi certificate** コマンドを使用します。

show platform sudi certificate [**sign** [**nonce** <*nonce*>]]

構文の説明

sign	（任意）署名を表示します。
nonce	（任意）ナンス値を入力します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

例

次に、特定の SUDI のチェックサム レコードを表示する例を示します。

```
Device# show platform sudi certificate

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQmqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBgNVBAoTBUNp
c2NvMRUwEwYDVQQDEwxBQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI5WhcNMjUw
ODA2MDgwODI5WjBzMSwwKgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNDhVWiBTTjpG
RE8xOTMyWDAwQzEOMAwGA1UEChMFQ2lzY28xGDAWBgNVBAsTD0FDVC0yIExpdGUg
U1VESTEZMBcGA1UEAxMQV1MtQzM2NTAtMTJYNDhVWjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANZxOGYI0eUl4HcSwjL4HO75qTjl9C2BHG3ufce9ikkN
xwGXi8qg8vKxuB9tRYRaJC5bP1WMoq7+ZJtQA079xE4X14soNbkq5NaUhh7RB1wD
```

```
iRUJvTfCOzVICbNfbzvtB30I75tCarFNmpd0K6AFrIa41U988QGqaCj7R1JrYNaj
nC73UXXM/hC0HtNR5mhyqer5Y2qjjzo6tHZYqrrx2eS1XOa262ZSQriAxmaH/KLC
K97ywyRBdJlxBRX3hGtKlog8nASB8WpXqB9NVCERzUajwU3L/kg2BsCqw9Y2m7HW
U1cerTxgthuyUkdNI+Jg6iGApm2+s8E9hsHPBPMCdIsCAwEAAaNvMG0wDgYDVR0P
AQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEEAQkVAgOg
NRMzQ2hpcElEPVVZSk5ORmRRRlFvN1ZIVmxJRTlqZENBeU9DQXhPRG93TlRveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbVCRjVIR5MQcWXUT086v6Ej
HahDHTts3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMUuoNL4szPhmmDcULfiCGBcA
/R3EFuoVMIzNT0geziytsCf728KGw1oGuosgVjNGOOahUELu4+F/My7bIJNbH+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d00Lm5L1WbBfQtyBaOLAbxsHvutrX
u1VZ5sdqSTwTkkO9vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfYfpiJ3cyJ0xf
I4brQ1smdczloFD4asF7A+1vor5e4VDBP0ppmeFAJvCQ52JTpj0M0o1D
-----END CERTIFICATE-----
```

show sdm prefer

特定の機能用のシステム リソースを最大にするために使用できる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。現在のテンプレートを表示するには、キーワードを指定せずにコマンドを使用します。

show sdm prefer [**advanced**]

構文の説明

advanced	（任意）高度なテンプレートに関する情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 コマンドを入力後にスイッチをリロードしていない場合、**show sdm prefer** 特権 EXEC コマンドでは、新しく設定されたテンプレートでなく現在使用中の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。たとえば、デバイスに 16 を超えるルーテッド インターフェイス（サブネット VLAN）がある場合、デ

フォルトのテンプレートでは、可能なユニキャスト MAC アドレスの数は 6000 未満になることがあります。

例

次に、**show sdm prefer** コマンドの出力例を示します。

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
 Number of VLANs:                                4094
 Unicast MAC addresses:                          32768
 Overflow Unicast MAC addresses:                 512
 IGMP and Multicast groups:                      8192
 Overflow IGMP and Multicast groups:             512
 Directly connected routes:                      32768
 Indirect routes:                                7680
 Security Access Control Entries:                3072
 QoS Access Control Entries:                     3072
 Policy Based Routing ACEs:                      1024
 Netflow ACEs:                                   1024
 Input Microflow policer ACEs:                   256
 Output Microflow policer ACEs:                  256
 Flow SPAN ACEs:                                 256
 Tunnels:                                        256
 Control Plane Entries:                          512
 Input Netflow flows:                            8192
 Output Netflow flows:                          16384
 SGT/DGT entries:                                4096
 SGT/DGT Overflow entries:                       512
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

Device#
```

関連トピック

sdm prefer, （1282 ページ）

show tech-support wireless

Cisco Technical Assistance Center（TAC）によって頻繁に要求されるシスコ ワイヤレス LAN コントローラの変数を表示するには、特権 EXEC モードで **show tech-support wireless** コマンドを使用します。

show tech-support wireless

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show tech-support wireless** コマンドの出力例を示します。

```
Device# show tech-support wireless
 *** show ap capwap timers ***

Cisco AP CAPWAP timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                             Retransmit Interval             Retransmit Count
-----------------------------------------------------------------------------------------------
TSIM_AP-2                           3                               5
TSIM_AP-3                           3                               5
*** show ap dot11 24ghz cleanair air-quality summary ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
                    0         0       0       0            No
*** show ap dot11 24ghz cleanair config ***

Clean Air Solution................................ : Disabled
Air Quality Settings:
    Air Quality Reporting......................... : Disabled
    Air Quality Reporting Period (min)............ : 15
    Air Quality Alarms............................ : Enabled
    Air Quality Alarm Threshold................... : 10
Interference Device Settings:
    Interference Device Reporting................. : Enabled
        Bluetooth Link............................ : Enabled
        Microwave Oven............................ : Enabled
        802.11 FH................................. : Enabled
        Bluetooth Discovery....................... : Enabled
        TDD Transmitter........................... : Enabled
        Jammer.................................... : Enabled
        Continuous Transmitter.................... : Enabled
        DECT-like Phone........................... : Enabled
        Video Camera.............................. : Enabled
        802.15.4.................................. : Enabled
        WiFi Inverted............................. : Enabled
        WiFi Invalid Channel...................... : Enabled
        SuperAG................................... : Enabled
        Canopy.................................... : Enabled
        Microsoft Device.......................... : Enabled
        WiMax Mobile.............................. : Enabled
        WiMax Fixed............................... : Enabled
    Interference Device Types Triggering Alarms:
```

```
        Bluetooth Link.......................... : Disabled
        Microwave Oven.......................... : Disabled
        802.11 FH............................... : Disabled
        Bluetooth Discovery..................... : Disabled
        TDD Transmitter......................... : Disabled
        Jammer.................................. : Disabled
        Continuous Transmitter.................. : Disabled
        DECT-like Phone......................... : Disabled
        Video Camera............................ : Disabled
  802.15.4.............................. : Disabled
        WiFi Inverted........................... : Enabled
        WiFi Invalid Channel.................... : Enabled
        SuperAG................................. : Disabled
        Canopy.................................. : Disabled
        Microsoft Device........................ : Disabled
        WiMax Mobile............................ : Disabled
        WiMax Fixed............................. : Disabled
    Interference Device Alarms.................. : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State............. : Disabled
    CleanAir Driven RRM Sensitivity............. : LOW
    CleanAir Persistent Devices state........... : Disabled
```

show wireless band-select

バンドセレクト設定のステータスを表示するには、特権 EXEC モードで **show wireless band-select** コマンドを使用します。

show wireless band-select

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless band-select** コマンドの出力例を示します。

```
Device# show wireless band-select
Band Select Probe Response    : per WLAN enabling
```

```
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : 80
```

show wireless client calls

デバイス のアクティブなコールまたは拒否されたコールの合計数を表示するには、特権 EXEC モードで **show wireless client calls** コマンドを使用します。

show wireless client calls {**active** | **rejected**}

構文の説明

active	アクティブなコールが表示されます。
rejected	拒否されたコールが表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless client calls** コマンドの出力例を示します。

```
デバイス# show wireless client calls active

TSPEC Calls:

-------------------------------------------------------------------------------
MAC Address     AP Name             Status               WLAN  Authenticated
-------------------------------------------------------------------------------
0000.1515.000f    AP-2           Associated             1   Yes

SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

特定の帯域（2.4 Ghz または 5 Ghz）のアクティブなコールまたは拒否されたコールの合計数を表示するには、特権 EXEC モードで **show wireless client dot11** コマンドを使用します。

show wireless client dot11 {**24ghz** | **5ghz**} **calls** {**active** | **rejected**}

構文の説明

24ghz	802.11b/g ネットワークを表示します。
5ghz	802.11a ネットワークを表示します。
calls	ワイヤレス クライアントのコールを表示します。
active	アクティブなコールが表示されます。
rejected	拒否されたコールが表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless client dot11** コマンドの出力例を示します。

```
Device# show wireless client dot11 5ghz calls active

 TSPEC Calls:
------------------


SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client location-calibration

ロケーション キャリブレーションを実行するために現在使用されているクライアントのリストを表示するには、特権 EXEC モードで **show wireless client location-calibration** コマンドを使用します。

show wireless client location-calibration

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless client location-calibration** コマンドの出力例を示します。

```
Device# show wireless client location-calibration
```

show wireless client probing

プロービング クライアントの数を表示するには、特権 EXEC モードで **show wireless client probing** コマンドを使用します。

show wireless client probing

構文の説明

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

特権 EXEC の動作や値はありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless client probing** コマンドの出力例を示します。

```
Device# show wireless client probing
MAC Address
------------------
000b.cd15.0001
000b.cd15.0002
000b.cd15.0003
000b.cd15.0004
000b.cd15.0005
000b.cd15.0006
```

show wireless client summary

コントローラと関連付けられているアクティブ クライアントの概要を表示するには、特権 EXEC モードで **show wireless client summary** コマンドを使用します。

show wireless client summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

次に、**show wireless client summary** コマンドの出力例を示します。

除外リスト（ブラック リスト）のクライアントを表示するには、**show wireless exclusionlist** コマンドを使用します。

```
Device# show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                          WLAN State              Protocol
-------------------------------------------------------------------------------
0000.1515.000f  AP-2                         1    UP                 11a
```

show wireless client timers

802.11 システム タイマーを表示するには、特権 EXEC モードで **show wireless client timers** コマンドを使用します。

show wireless client timers

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless client timers** コマンドの出力例を示します。

```
Device# show wireless client timers
 Authentication Response Timeout (seconds)      : 10
```

show wireless client voice diagnostics

ワイヤレス クライアントの音声診断パラメータを表示するには、特権 EXEC モードで **show wireless client voice diagnostics** コマンドを使用します。

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rssi** | **status** | **tspec**}

構文の説明

qos-map	QoS および DSCP マッピングに関する情報と 4 つのキュー（VO、VI、BE、BK）それぞれのパケット統計を表示します。各種 DSCP 値も表示されます。
roam-history	既知の各クライアントの直前の 3 つのローミング履歴に関する情報を表示します。出力にはタイムスタンプ、ローミングに関連するアクセスポイント、ローミングの理由が含まれ、ローミングに失敗した場合には失敗の理由も含まれます。
rssi	音声診断がイネーブルである場合に、直前の 5 秒間のクライアントの RSSI 値を表示します。
status	クライアントの音声診断の状態を表示します。
tspec	TSPEC クライアントに対して有効になっている音声診断を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デバッグ音声診断は、音声診断を実行するにはイネーブルにする必要があります。

次は、**show wireless client voice diagnostics status** コマンドの出力例です。

```
Device# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show wireless country

サポートされる設定済みの国タイプと無線タイプを表示するには、特権 EXEC モードで **show wireless country** コマンドを使用します。

show wireless country {channels| configured| supported [tx-power]}

構文の説明

channels	帯域ごとに使用可能なチャネルのリストと、設定されている国で許容されるチャネルのリストを表示します。
configured	設定されている国を表示します。
supportedtx-power	サポートされている各国で許容される Tx 電源のリストを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless country channels** コマンドの出力例を示します。

```
Device# show wireless country channels
  Configured Country.............................: US  - United States
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    802.11bg     :
    Channels     :                   1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US  :  A * * * * A * * * * A . . .
 Auto-RF         : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11a         :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 Channels        : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                 : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US  :  . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 4.9GHz 802.11a  :
   Channels      :                   1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-A   ,-AB  ): * * * * * * * * * * * * * * * * * * * A * * * * * A
```

```
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

次に、**show wireless country configured** コマンドの出力例を示します。

```
Device# show wireless country configured
 Configured Country.............................: US  - United States
 Configured Country Codes
        US  - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

次に、**show wireless country supported tx-power** コマンドの出力例を示します。

```
Device# show wireless country supported tx-power
      KEY: ##    = Tx Power in dBm.
           ##*   = Channel supports radar detection .
           .     = Channel is not legal in this country.
           (-)   = Regulatory Domains allowed by this country.
           (-,-) = (indoor, outdoor) regulatory Domains allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    802.11bg     :
    Channels     :                   1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-CE  ,-CE  )  AE  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  AL  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  AR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  AT  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-NA  )  AU  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BA  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  BE  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  BG  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-    )  BH  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-A   )  BO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-AR  )  BR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BY  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  CA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-ABN )  CA2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  CH  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-AER ,-AR  )  CL  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  CM  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-CE  ,-CE  )  CN  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  CO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-AB  )  CR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  CY  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  CZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  DE  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  DK  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  DO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  DZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AB  )  EC  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  EE  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  EG  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  ES  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  FI  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  FR  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GB  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GI  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GR  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-NA  )  HK  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  HR  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  HU  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-ER  )  ID  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  IE  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-EI  ,-IE  )  IL  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-I   ,-I   )  ILO :   .  .  .  . 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AN  )  IN  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  IQ  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  IS  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  IT  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-JPU ,-JPU )  J2  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
 (-JPU ,-JPU )  J3  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
```

```
(-JPQU,-PQ  )  J4  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E   ,-    )  JO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  JP  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE ,-ACEK)  KE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-ACE ,-ACEK)  KR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KW  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  LK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LV  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MC  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ME  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  MO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  MX  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-ACE ,-AEC )  MY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  NZ  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  OM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AR  )  PA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  PE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  PL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  QA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AER ,-ER  )  RU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AE  ,-AE  )  SA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-SE  )  SG  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E   ,-E   )  SI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-ER  )  TH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  TN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-EI  ,-E   )  TR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-ANT )  TW  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  UA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AB  )  US  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  US2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  USL :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-    )  USX :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-A   )  UY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  VE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  VN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ZA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

show wireless detail

設定済みのワイヤレス パラメータの詳細を表示するには、特権 EXEC モードで **show wireless detail** コマンドを使用します。

show wireless detail

構文の説明

特権 EXEC の動作引数はありません。

コマンド デフォルト

デフォルトはありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

次のようなパラメータが表示されます。

- ワイヤレス ユーザ アイドル タイムアウト
- コントローラで設定されている RF グループ名
- Fast SSID change

次に、**show wireless detail** コマンドの出力例を示します。

```
Device# show wireless detail
User Timeout               : 300
RF network                 : default
Fast SSID                  : Disabled
```

show wireless dtls connections

Datagram Transport Layer Security（DTLS）サーバのステータスを表示するには、特権 EXEC モードで **show wireless dtls connections** コマンドを使用します。

show wireless dtls connections

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless dtls connections** コマンドの出力例を示します。

```
Device# show wireless dtls connections
 AP Name         Local Port   Peer IP    Peer Port  Ciphersuite
------------------------------------------------------------------------
  AP-2       Capwap_Ctrl   10.0.0.16     52346      TLS_RSA_WITH_AES_128_CBC_SHA
  AP-3       Capwap_Ctrl   10.0.0.17     52347      TLS_RSA_WITH_AES_128_CBC_SHA
```

show wireless flow-control

特定のチャネルのフロー制御に関する情報を表示するには、特権 EXEC モードで **show wireless flow-control** コマンドを使用します。

show wireless flow-control *channel-id*

構文の説明

channel-id	フロー制御がモニタされるチャネルの識別番号。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show wireless flow-control** *channel-id* コマンドの出力例を示します。

```
Device# show wireless flow-control 3
Channel Name                          : CAPWAP
FC State                              : Disabled
```

```
Remote Server State                    : Enabled
Pass-thru Mode                         : Disabled
EnQ Disabled                           : Disabled
Queue Depth                            : 2048
Max Retries                            : 5
Min Retry Gap (mSec)                   : 3
```

show wireless flow-control statistics

特定のチャネルのフロー制御に関する完全な情報を表示するには、特権 EXEC モードで **show wireless flow-control statistics** コマンドを使用します。

show wireless flow-control *channel-id* **statistics**

構文の説明

channel-id	フロー制御がモニタされるチャネルの識別番号。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show wireless flow-control** *channel-id* **statistics** コマンドの出力例を示します。

```
Device# show wireless flow-control 3 statistics
 Channel Name                                : CAPWAP
# of times channel went into FC              : 0
# of times channel came out of FC            : 0
Total msg count received by the FC Infra     : 1
Pass-thru msgs send count                    : 0
Pass-thru msgs fail count                    : 0
# of msgs successfully queued                : 0
# of msgs for which queuing failed           : 0
# of msgs sent thru after queuing            : 0
# of msgs sent w/o queuing                   : 1
# of msgs for which send failed              : 0
# of invalid EAGAINS received                : 0
Highest watermark reached                    : 0
# of times Q hit max capacity                : 0
Avg time channel stays in FC (mSec)          : 0
```

show wireless load-balancing

ロード バランシング機能のステータスを表示するには、特権 EXEC モードで **show wireless load-balancing** コマンドを使用します。

show wireless load-balancing

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless load-balancing** コマンドの出力例を示します。

```
 > show wireless load-balancing
Aggressive Load Balancing.........................: per WLAN enabling
Aggressive Load Balancing Window (clients).................:: 5
Aggressive Load Balancing Denial Count.....................:: 3

Statistics
Total Denied Count (clients)...............................:: 0
Total Denial Sent (messages)...............................:: 0
Exceeded Denial Max Limit Count (times)....................:: 0
None 5G Candidate Count (times)............................:: 0
None 2.4G Candidate Count (times)..........................:: 0
```

show wireless performance

アグレッシブ ロード バランシングの設定を表示するには、特権 EXEC モードで **show wireless performance** コマンドを使用します。

show wireless performance {ap| client}summary

構文の説明

apsummary	コントローラに対して設定されているアクセス ポイントのアグレッシブ ロード バランシングの設定を表示します。
client summary	クライアントのアグレッシブ ロード バランシングの設定の詳細を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless performance ap summary** コマンドの出力例を示します。

```
Device# show wireless performance ap summary
Number of APs:
```

次に、**show wireless performance client summary** コマンドの出力例を示します。

```
Device# show wireless performance client summary
Number of Clients:

MAC Address        AP Name           Status        WLAN/Guest-Lan Auth Protocol Port Wired
-------------------------------------------------------------------------------------------
```

show wireless pmk-cache

ペアワイズ マスター キー（PMK）キャッシュに関する情報を表示するには、特権 EXEC モードで **show wireless pmk-cache** コマンドを使用します。

show wireless pmk-cache[**mac-address** *mac-addr*]

構文の説明

mac-address*mac-addr*	（任意）PMK キャッシュの単一エントリに関する情報。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless pmk-cache mac-address** コマンドの出力例を示します。

```
Device# show wireless pmk-cache mac-address H.H.H
Number of PMK caches in total : 0
```

show wireless probe

拡張プローブ要求フィルタリングの設定と、各クライアントのアクセス ポイントごとの WLAN コントローラに送信されたプローブ数およびプローブ間隔（ミリ秒）を表示するには、特権EXEC モードで **show wireless probe** コマンドを使用します。

show wireless probe

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless probe** コマンドの出力例を示します。

```
Device# show wireless probe
Probe request filtering                          : Enabled
Number of probes per client per radio fwd from AP: 2
Probe request rate-limiting interval             : 500 msec
Aggregate probe request interval                 : 500 msec
```

show wireless sip preferred-call-no

SIP 優先コール番号を表示するには、特権 EXEC モードで **show wireless sip preferred-call-no** コマンドを使用します。

show wireless sip preferred-call-no

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless sip preferred-call-no** コマンドの出力例を示します。

```
Device# show wireless sip preferred-call-no
Index Preferred-Number
----------------------
1     1031
2     1032
```

```
4     1034
```

show wireless summary

コントローラに認識されているアクセスポイント、無線クライアントとワイヤレスクライアントの数を表示するには、特権 EXEC モードで **show wireless summary** コマンドを使用します。

show wireless summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、**show wireless summary** コマンドの出力例を示します。

```
Device# show wireless summary

Access Point Summary

               Total    Up    Down
-------------------------------------
802.11a/n          2     2       0
802.11b/g/n        2     2       0
All APs            2     2       0

Client Summary

Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

shutdown

VLAN スイッチングをシャットダウンするには、グローバル コンフィギュレーション モードで **shutdown** コマンドを使用します。設定セットをディセーブルにするには、このコマンドの **no** 形式を使用します。

shutdown [**vlan** *vlan-id*]

no shutdown

構文の説明

vlan *vlan-id*	シャットダウンする VAN の VLAN ID。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

例

次に、VLAN をシャットダウンする方法の例を示します。

```
Device(config)# vlan open1
Device(config-wlan)# shutdown
```

次に、アクセス ポイントがシャットダウンされない例を示します。

```
Device# configure terminal
Device(config)# ap name 3602a no shutdown
```

system env temperature threshold yellow

イエローのしきい値を決定する、イエローとレッドの温度しきい値の差を設定するには、グローバル コンフィギュレーション コマンドで **system env temperature threshold yellow** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

system env temperature threshold yellow *value*

no system env temperature threshold yellow *value*

構文の説明

value	イエローとレッドのしきい値の差を指定します（摂氏）。指定できる範囲は 10 ～ 25 です。

コマンド デフォルト

デフォルト値は次のとおりです。

表 *53*：温度しきい値のデフォルト値

Device	イエローとレッドの差	レッド[13]
Catalyst 3850	14 °C	60 °C

13 レッドの温度しきい値を設定することはできません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

グリーンとレッドのしきい値を設定することはできませんが、イエローのしきい値を設定することはできます。イエローとレッドのしきい値の差を指定して、イエローのしきい値を設定するには、**system env temperature threshold yellow***value* グローバル コンフィギュレーション コマンドを使用します。たとえば、レッドのしきい値が 66 □であり、イエローのしきい値を 51 □に設定するには、**system env temperature threshold yellow 15** コマンドを使用してしきい値の差を 15 に設定します。たとえば、レッドのしきい値が 60 □であり、イエローのしきい値を 51 □に設定するには、**system env temperature threshold yellow 9** コマンドを使用してしきい値の差を 9 に設定します。

（注） デバイス内部の温度センサーでシステム内の温度を測定するため、±5 °Cの差が生じる可能性があります。

例

次の例では、イエローとレッドのしきい値の差を 15 に設定する方法を示します。

```
Device(config)# system env temperature threshold yellow 15
Device(config)#
```

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

interface-id	TDR を実行するインターフェイス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 は、銅線のイーサネット 10/100/100 ポートだけでサポートされます。10 ギガビット イーサネット ポートまたは Small Form-Factor Pluggable（SFP）モジュール ポートではサポートされません。

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。

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。

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
```

```
Use 'show cable-diagnostics tdr' to read the TDR results
```

インターフェイスのリンク ステータスがアップ状態で速度が 10 Mb/s または 100 Mb/s である場合、**test cable-diagnostics tdr interface***interface-id* コマンドを入力すると、次のメッセージが表示されます。

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

関連トピック

show cable-diagnostics tdr, （1288 ページ）

traceroute mac

指定の送信元 MAC アドレスから指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示するには、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

interface*interface-id*	（任意）送信元または宛先デバイス上のインターフェイスを指定します。
source-mac-address	送信元デバイスの 16 進形式の MAC アドレス。
destination-mac-address	宛先デバイスの 16 進形式の MAC アドレス。
vlan*vlan-id*	（任意）送信元デバイスから宛先デバイスまでをパケットが通過するレイヤ 2 のパスをトレースする VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。
detail	（任意）詳細情報を表示するよう指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 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デバイスで有効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。

デバイスがレイヤ 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、デバイスはレイヤ 2 trace クエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 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 に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。

VLAN を指定しないと、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。

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

次の例では、**detail** キーワードを使用することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201 detail
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 / WS-C3750E-24PD / 2.2.6.6 :
          Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
  con5 / WS-C2950G-24-EI / 2.2.5.5 :
          Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

次の例では、送信元および宛先デバイス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。

```
Device# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

次の例では、デバイスが送信元デバイスに接続されていない場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
          Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

次の例では、デバイスが送信元 MAC アドレスの宛先ポートを検出できない場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
  Error:Source Mac address not found.
  Layer2 trace aborted.
```

次の例では、送信元および宛先デバイスが異なる VLAN にある場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
  Error:Source and destination macs are on different vlans.
  Layer2 trace aborted.
```

次の例では、宛先MACアドレスがマルチキャストアドレスの場合のレイヤ2のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
  Invalid destination mac address
```

次の例では、送信元および宛先デバイスが複数の VLAN にある場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Error:Mac found on multiple vlans.
  Layer2 trace aborted.
```

関連トピック

traceroute mac ip, （1342 ページ）

traceroute mac ip

指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示するには、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

source-ip-address	32 ビットの値（ドット付き 10 進表記）で指定された送信元デバイスの IP アドレス。
source-hostname	送信元デバイスの IP ホスト名。
destination-ip-address	32 ビットの値（ドット付き 10 進表記）で指定された宛先デバイスの IP アドレス。
destination-hostname	宛先デバイスの IP ホスト名。
detail	（任意）詳細情報を表示するよう指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 の traceroute を適切に機能させるには、Cisco Discovery Protocol（CDP）がネットワークの各デバイス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。

デバイスがレイヤ 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、デバイスはレイヤ 2 trace クエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 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、デバイスは Address Resolution Protocol（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 を対応させます。

- 指定の IP アドレスの ARP のエントリが存在している場合、デバイスは対応する MAC アドレスを使用して、物理パスを識別します。
- ARP のエントリが存在しない場合、デバイスは ARP クエリを送信し、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場合は、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、送信元と宛先の 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。

```
Device# 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 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
```

```
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# 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) :Gi0/0/1 => Gi0/0/3
con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
con2                (2.2.2.2        )  :    Gi0/0/2 => 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。

```
Device# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

関連トピック

traceroute mac, （1339 ページ）

trapflags

不正アクセス ポイント検出トラップの送信を有効にするには、特権 EXEC モードで **trapflags** コマンドを使用します。不正アクセス ポイント検出トラップの送信を無効にするには、このコマンドの **no** 形式を使用します。

trapflags rogueap

no trapflags rogueap

構文の説明

rogueap	不正アクセス ポイント検出トラップの送信を有効にします。

コマンド デフォルト

コマンド モード

イネーブル
特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、不正なアクセス ポイント検出トラップの送信をディセーブルにする例を示します。

```
Device# configure terminal
Device(config)# no trapflags rogueap
Device(config)# end
```

trapflags client

クライアント関連のDOT11トラップの送信を有効にするには、特権EXECモードで**trapflags client**コマンドを使用します。クライアント関連のDOT11トラップの送信を無効にするには、このコマンドの **no** 形式を使用します。

trapflags client [**dot11** {**assocfail**| **associate**| **authfail**| **deauthenticate**| **disassociate**}| **excluded**]

no trapflags client [**dot11** {**assocfail**| **associate**| **authfail**| **deauthenticate**| **disassociate**}| **excluded**]

構文の説明

dot11	クライアント関連の DOT11 トラップ。
assocfail	クライアントへの Dot11 アソシエーション エラー トラップの送信をイネーブルにします。
associate	クライアントへの Dot11 アソシエーション トラップの送信をイネーブルにします。
authfail	クライアントへの Dot11 認証エラー トラップの送信をイネーブルにします。
deauthenticate	クライアントへの Dot11 認証解除トラップの送信をイネーブルにします。
disassociate	クライアントへの Dot11 ディスアソシエーション トラップの送信をイネーブルにします。
excluded	除外したトラップのクライアントへの送信をイネーブルにします。

コマンド デフォルト

特権 EXEC の動作や値はありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、クライアントへの Dot11 アソシエーション解除トラップの送信をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# trapflags client dot11 disassociate
Device(config)# end
```

type

一つ以上のファイルの内容を表示するには、ブートローダ モードで **type** コマンドを使用します。

type*filesystem:/file-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリ スティックには **usbflash0:** を使用します。
/file-url...	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。

ファイルのリストを指定すると、各ファイルの内容が順次表示されます。

例

次に、ファイルの内容を表示する例を示します。

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

unset

1 つ以上の環境変数をリセットするには、ブート ローダ モードで **unset** 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**：デバイスの起動を自動で行うか手動で行うかどうかを指定します。
	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 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。
	ENABLE_BREAK：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指定します。
	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を識別します。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。
	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する文字列を指定します。
	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（b/s）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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**no boot manual** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

BOOT 環境変数は、**no boot system** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

ENABLE_BREAK 環境変数は、**no boot enable-break** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

HELPER 環境変数は、**no boot helper** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

CONFIG_FILE 環境変数は、**no boot config-file** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

例

次に、SWITCH_PRIORITY 環境変数をリセットする例を示します。

```
Device: unset SWITCH_PRIORITY
```

関連トピック

セット，（1283 ページ）

reset, （1280 ページ）

version

ブートローダのバージョンを表示するには、ブート ローダ モードで **version** コマンドを使用します。

version

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

例

次に、デバイスのブート ローダのバージョンを表示する例を示します。

```
Device: version
CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 1.3, RELEASE SOFTWARE (P)
Compiled Sun Jun 16 18:31:15 PDT 2013 by rel
```

wireless client

クライアント 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 **wirelessclient** コマンドを使用します。

wireless client {**association limit** *assoc-number* **interval** *interval*| **band-select** {**client-rssi** *rssi*| **cycle-count** *count*| **cycle-threshold** *threshold*| **expire dual-band** *timeout*| **expire suppression** *timeout*}| **max-user-login** *max-user-login*| **timers auth-timeout** *seconds*| **user-timeout** *user-timeout*}

構文の説明

associationlimit*assoc-number***interval***interval*	所定の間隔での 1 つのアクセス ポイント スロットあたりの関連付け要求制限を有効にし、関連付け要求制限間隔を設定します。 所定の間隔での 1 つのアクセス ポイント スロットあたりの関連付け要求の数は、1～100 の範囲で設定できます。 クライアント関連付け要求制限間隔は、100～10000 ミリ秒の範囲で設定できます。
band-select	クライアントのバンド選択オプションを設定します。
client-rssi*rssi*	バンド選択のクライアント受信信号強度インジケータ（RSSI）しきい値を設定します。 -90 ～ -20 のプローブに応答するクライアント RSSI の最小 dBm。
cycle-count*count*	バンド選択プローブ周期カウントを設定します。 周期カウントは、1～10 の範囲で設定できます。
cycle-threshold*threshold*	新規スキャン周期の時間しきい値を設定します。 周期しきい値は、1～1000 ミリ秒の範囲で設定できます。
expiredual-band*timeout*	特定のクライアントを 5 GHz 帯域にプッシュする試行を停止するまでのタイムアウトを設定します。 タイムアウトは 10 ～ 300 秒の範囲で設定できます。デフォルト値は 60 秒です。
expiresuppression*timeout*	既知のデュアルバンドクライアントが失効してプルーニングされるまでの時間を設定します。 抑止時間は 10～200 秒の範囲で設定できます。デフォルトのタイムアウト値は 20 秒です。
max-user-login*max-user-login*	ユーザのログインセッションの最大数を設定します。
timersauth-timeout*seconds*	クライアント タイマーを設定します。
user-timeout*user-timeout*	アイドル クライアント タイムアウトを設定します。

コマンド デフォルト

グローバルの動作や値はありません。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、帯域幅選択のプローブ サイクルカウントを 8 に設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 8
Device(config)# end
```

次に、しきい値が 700 ミリ秒の新しいスキャン サイクルの時間のしきい値を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select cycle-threshold 700
Device(config)# end
```

次に、70 秒後にデュアルバンド データベースのデュアルバンド クライアントを抑止する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 70
Device(config)# end
```

wireless client mac-address deauthenticate

ワイヤレス クライアントへの接続を解除するには、グローバル コンフィギュレーション モードで **wireless client mac-address deauthenticate** コマンドを使用します。

wirelessclientmac-address *mac-addr***deauthenticate**

構文の説明

mac-address *mac-addr*	ワイヤレス クライアントの MAC アドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、ワイヤレス クライアントを接続解除する例を示します。

```
Device# configure terminal
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 deauthenticate
Device(config)# end
```

wireless client mac-address

ワイヤレス クライアントの設定を構成するには、グローバル コンフィギュレーション モードで **wirelessclientmac-address** コマンドを使用します。

wireless client mac-address *mac-addr* **ccx** {**clear-reports**| **clear-results**| **default-gw-ping**| **dhcp-test**| **dns-ping**| **dns-resolve hostname** *host-name*| **get-client-capability**| **get-manufacturer-info**| **get-operating-parameters**| **get-profiles**| **log-request** {**roam**| **rsna**| **syslog**}| **send-message** *message-id*| **stats-request** *measurement-duration* {**dot11**| **security**}| **test-abort**| **test-association** *ssid bssid dot11 channel*| **test-dot1x** [*profile-id*] *bssid dot11 channel*| **test-profile** {**any**| *profile-id*}}

構文の説明

mac-addr	クライアントの MAC アドレス。
ccx	Cisco Client Extension（CCX）。
clear-reports	クライアント レポートの情報をクリアします。
clear-results	コントローラのテスト結果をクリアします。
default-gw-ping	デフォルト ゲートウェイ ping テストの実行要求をクライアントに送信します。
dhcp-test	DHCP テストの実行要求をクライアントに送信します。
dns-ping	ドメイン ネーム システム（DNS）サーバ IP アドレス ping テストの実行要求をクライアントに送信します。
dns-resolvehostname*host-name*	指定されたホスト名に対するドメイン ネーム システム（DNS）解決テストの実行要求をクライアントに送信します。

get-client-capability	クライアントにその機能情報を送信するよう指示する要求を送信します。
get-manufacturer-info	製造元の情報を送信するよう指示する要求をクライアントに送信します。
get-operating-parameters	クライアントに現在の動作パラメータを送信するよう指示する要求を送信します。
get-profiles	クライアントにプロファイルを送信するよう指示する要求を送信します。
log-request	指定されたクライアント デバイスに対する CCX ログ要求を設定します。
roam	（任意）クライアント CCX ローミング ログを指定する要求を指定します。
rsna	（任意）クライアント CCX RSNA ログを指定する要求を指定します。
syslog	（任意）クライアント CCX システム ログを指定する要求を指定します。

send-message*message-id*

メッセージをクライアントに送ります。

次のいずれかを含むメッセージ タイプ。

- 1：SSID が無効です。
- 2：ネットワーク設定が無効です。
- 3：WLAN の信頼性に不一致があります。
- 4：ユーザの資格情報が間違っています。
- 5：サポートにお問い合わせください。
- 6：問題は解決されました。
- 7：問題は解決されていません。
- 8：もう一度後で作業を行ってください。
- 9：示された問題を修正してください。
- 10：ネットワークにより、トラブルシューティングが拒否されました。
- 11：クライアント レポートを取得中です。
- 12：クライアント ログを取得中です。
- 13：取得が完了しました。
- 14：アソシエーション テストを開始します。
- 15：DHCP テストを開始します。
- 16：ネットワーク接続テストを開始します。
- 17：DNS ping テストを開始します。
- 18：名前解決テストを開始します。
- 19：802.1X 認証テストを開始します。
- 20：クライアントを特定のプロファイルにリダイレクトしています。
- 21：テストが完了しました。
- 22：テストに合格しました。
- 23：テストに失敗しました。
- 24：通常の操作を再開するには、診断チャネル操作をキャンセルするか、WLANプロファイルを選択してください。
- 25：クライアントにより、ログの取得が拒否されました。

- 26：クライアントにより、クライアント レポートの取得が拒否されました。
- 27：クライアントにより、テスト要求が拒否されました。
- 28：無効なネットワーク（IP）設定です。
- 29：ネットワークで機能停止または問題が発生しています。
- 30：予定された保守期間です。
- 31：WLAN セキュリティ方式が正しくありません。
- 32：WLAN 暗号化方式が正しくありません。
- 33：WLAN 認証方式が正しくありません。

stats-request*measurement-duration*	統計情報の要求を送信します。
dot11	（任意）dot11 カウンタを指定します。
security	（任意）セキュリティ カウンタを指定します。
test-abort	現在のテストを中止するよう指示する要求をクライアントに送信します。
test-association*ssidbssiddot11channel*	関連付けテストの実行要求をクライアントに送信します。
test-dot1x	802.1x テストの実行要求をクライアントに送信します。
profile-id	（任意）テストのプロファイル名。
bssid	Basic SSID。
dot11	802.11a、802.11b、または 802.11g ネットワークを指定します。
channel	チャネル番号。
test-profile	プロファイル リダイレクト テストの実行要求をクライアントに送信します。
any	プロファイル リダイレクト テストの実行要求をクライアントに送信します。

profile-id	テスト プロファイル名。 （注） プロファイル ID には、必ずクライアント レポートが有効なクライアント プロファイルのプロファイル ID を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

default-gw-ping テストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアントの MAC アドレス 00:1f:ca:cf:b6:60 のレポート情報をクリアする例を示します。

```
Device# configure terminal
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Device(config)# end
```

wireless load-balancing

コントローラでアグレッシブ ロードバランシ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 **wirelessload-balancing** を使用します。

wireless load-balancing {**denial** *denial-count*| **window** *client-count*}

構文の説明

denial*denial-count*	ロード バランシング時に拒否されるアソシエーションの数を指定します。 ロード バランシング時の関連付け拒否の最大数は、1 ~ 10 の範囲で指定できます。デフォルト値は 3 です。

window*client-count*	アグレッシブ ロード バランシング クライアント ウィンドウと、特定のアクセス ポイントに対するアグレッシブ ロード バランシングをトリガーするのに必要なクライアント数を指定します。 クライアント数を指定したアグレッシブ ロード バランシング クライアント ウィンドウは、0 ~ 20 の範囲で指定できます。デフォルト値は 5 です。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

負荷分散が有効になっているWLANは、音声およびビデオなどの時間依存型アプリケーションをサポートしません。これは、ローミングでの遅延が存在するためです。

コントローラとともに Cisco 7921 および 7920 Wireless IP Phone を使用する場合、各コントローラの音声 WLAN でアグレッシブなロード バランシングが無効化されていることを確認します。無効化されていない場合、電話による初期ローミングが失敗し、オーディオ パスが中断されることがあります。

次に、ロード バランシング中の関連付け拒否を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless load-balancing denial 5
Device(config)# end
```

wireless sip preferred-call-no

新しい優先コールを追加したり、音声優先制御を設定したりするには、グローバル コンフィギュレーション モードで **wirelesssippreferred-call-no** コマンドを使用します。優先コールを削除するには、このコマンドの **no** 形式を使用します。

wireless sip preferred-call-no *callIndex call-no*

no wireless sip preferred-call-no *callIndex*

構文の説明

callIndex	1 ～ 6 の間の有効な値を持つコール インデックス。
call-no	27 文字まで使用できる優先コール数。

コマンド デフォルト

デフォルトの動作や値はありません。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

音声優先制御を設定する前に、次の前提条件を実行する必要があります。

- 音声コールがパススルーできるように WLAN QoS を設定します。
- 無線の ACM を有効にします。
- WLAN 上で SIP コール スヌーピングを有効にします。

次に、新しい優先コールを追加するか、または音声優先制御を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless sip preferred-call-no 2 0123456789
Device(config)# end
```

第 22 章

自律型ネットワーキング コマンド

- autonomic adjacency-discovery, 1361 ページ
- autonomic connect, 1362 ページ
- clear autonomic, 1363 ページ
- debug autonomic, 1365 ページ
- show autonomic control-plane, 1366 ページ
- show autonomic device, 1367 ページ
- show autonomic interfaces, 1368 ページ
- show autonomic intent, 1369 ページ
- show autonomic l2-channels, 1370 ページ
- show autonomic service, 1371 ページ
- show autonomic neighbor, 1372 ページ

autonomic adjacency-discovery

インターフェイスで隣接関係探索（ネイバー探索）を有効にするには、インターフェイス コンフィギュレーション モードで **autonomic adjacency-discovery** コマンドを使用します。隣接関係探索を無効にするには、このコマンドの **no** 形式を使用します。

autonomic adjacency-discovery

no autonomic adjacency-discovery

コマンド デフォルト

隣接関係探索は有効になっていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、隣接関係探索を有効にする例を示します。

```
デバイス(config)#  interface Tunnel100
デバイス(config-if)#  autonomic adjacency-discovery
```

autonomic connect

非自律型デバイスを自律型ドメインに接続するには、インターフェイス コンフィギュレーション モードで**autonomic connect**コマンドを使用します。デバイスをドメインから切断するには、このコマンドの **no** 形式を使用します。

autonomic connect

no autonomic connect

コマンド デフォルト

デバイスがドメインに接続されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

autonomic connectコマンドを実行するには、インターフェイスで**no switchport**を設定する必要があります。

次に、非自律型デバイスを自律型ドメインに接続する例を示します。

```
デバイス > enable
デバイス# configure terminal
デバイス(config)# int gig 1/0/1
デバイス(config-if)# no switchport
```

```
デバイス(config-if)# autonomic connect
デバイス(config-if)# ipv6 address 5000::1/64
```

clear autonomic

自律型ネットワークに関する情報をクリアまたはリセットするには、特権EXECコンフィギュレーション モードで **clear autonomic** コマンドを使用します。

clear autonomic {**device**| **neighbor** *neighbor's UDI*| **registrar accepted-device** *device UDI*}

構文の説明

デバイス	デバイス情報をクリアまたはリセットします。
neighbor*udi*	ネイバー情報をクリアまたはリセットします。
registrar accepted-device*udi*	各登録済みデバイスの保存されている公開キーをクリアします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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 autonomic device コマンドは、自律型ネットワークに関するデバイス固有の情報のすべてをクリアまたはリセットします（ブートストラップ プロセスで取得した情報を含みます）。**clear autonomic neighbor** コマンドは、ネイバー探索時に取得したネイバーに関する情報をクリアします。ネイバーを指定しない場合は、ネイバー データベース全体がクリアされます。**clear registrar accepted-device** コマンドは、レジストラに登録された各デバイスの保存されている公開キーをクリアします。

次に、自律型ネットワークに関するデバイス固有の情報のすべてをクリアする例を示します。

```
デバイス #clear autonomic device
```

```
% invoke syslog_an_delete_host: vrf cisco_autonomic
discriminator
Device#
Jul 15 05:55:53.987: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:55:53.988: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:55:53.990: %AN-6-ACP_DIKE_TO_NBR_REMOVED: Removed DIKE on ACP Tunnel100000 from
Device (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:7) to Neighbor (Addr
FD08:2EEF:C2EE:0:E865:493B:ACFB:5) connected on interface GigabitEthernet1/0/3
Jul 15 05:55:54.006: %AN-6-ACP_CHANNEL_TO_NBR_REMOVED: Removed ACP Tunnel100000 from Device
 (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:7) to Neighbor (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:5)
 connected on interface GigabitEthernet1/0/3
Jul 15 05:55:54.015: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:55:54.016: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback100000, changed
 state to down
Jul 15 05:55:54.097: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:55:54.104: %AN-5-NBR_LOST: Device with ACP (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:7)
 lost connectivity to its Neighbor (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:5) on interface
GigabitEthernet1/0/3
Jul 15 05:55:54.113: %AN-5-CD_STATE_CHANGED: L2 Channel (0) Removed - Our Intf
(GigabitEthernet1/0/3), Nbr UDI (PID:WS-C3850-24U SN:FCW1934D05Z), Nbr Intf
(GigabitEthernet1/0/3)
Jul 15 05:55:56.004: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100000, changed
 state to down
Jul 15 05:55:56.005: %LINK-5-CHANGED: Interface Tunnel100000, changed state to
administratively down
Jul 15 05:56:04.128: %AN-6-UDI_AVAILABLE: UDI - PID:WS-C3650-24TD SN:FDO1942E1YK
Jul 15 05:56:36.306: %AN-5-CD_STATE_CHANGED: L2 Channel (0) Created - Our Intf
(GigabitEthernet1/0/3), Nbr UDI (PID:WS-C3850-24U SN:FCW1934D05Z), Nbr Intf
(GigabitEthernet1/0/3)
Jul 15 05:56:36.310: %LINK-3-UPDOWN: Interface ANI1, changed state to up
Jul 15 05:56:37.294: %LINEPROTO-5-UPDOWN: Line protocol on Interface ANI1, changed state
to up
Jul 15 05:56:44.138: %AN-5-NBR_ADDED: Device with UDI (PID:WS-C3850-24U SN:FCW1934D05Z) is
 added as a Neighbor to Device with (Addr UNKNOWN) on the interface GigabitEthernet1/0/3
Jul 15 05:56:44.146: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.148: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.150: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.247: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.258: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.269: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:04.897: %CRYPTO-6-AUTOGEN: Generated new 3072 bit key pair
Jul 15 05:57:05.359: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:05.815: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:05.817: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:05.830: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:05.840: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:05.841: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.308: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:06.311: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.313: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.314: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.810: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.811: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:06.811: %AN-5-DEVICE_BOOTSTRAPPED_BY_ANR: Device with UDI (PID:WS-C3650-24TD
SN:FDO1942E1YK) and (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:7) has been boot trapped by
autonomic registrar, in autonomic domain cisco.com
Jul 15 05:57:06.815: %AN-6-ACP_VRF_GLOBAL_CREATE_SUCCESS: Device UDI (PID:WS-C3650-24TD
SN:FDO1942E1YK) Autonomic VRF created globally vrf name cisco_autonomic, vrf id 3
Jul 15 05:57:06.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback100000, changed
 state to up
Jul 15 05:57:06.828: %AN-6-ACP_VRF_INTERFACE_CREATE_SUCCESS: Device UDI (PID:WS-C3650-24TD
 SN:FDO1942E1YK) Autonomic VRF created successfully on interface Loopback100000, vrf name
cisco_autonomic, vrf id 3
Jul 15 05:57:06.837: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.840: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.842: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.842: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
```

```
memory" to save new IOS PKI configuration
Jul 15 05:57:07.905: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100001, changed
 state to up
Jul 15 05:57:08.159: %CRYPTO-6-IKMP_NO_ID_CERT_ADDR_MATCH: (NOT ERROR BUT WARNING ONLY)ID
of FE80::3A20:56FF:FEF3:7158 (type 5) and certificate addr with
Jul 15 05:57:08.160: %CRYPTO-6-IKMP_NO_ID_CERT_ADDR_MATCH: (NOT ERROR BUT WARNING ONLY)ID
of FE80::3A20:56FF:FEF3:7158 (type 5) and certificate addr with
Jul 15 05:57:11.959: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:11.960: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:11.963: %SYS-5-CONFIG_I: Configured from console by console
```

debug autonomic

自律型ネットワークに関する情報のデバッグを有効にするには、特権 EXEC モードで **debug autonomic** コマンドを使用します。デバッグを停止するには、このコマンドの **no** 形式を使用します。

debug autonomic{**Bootstrap**| **Channel-Discovery**| **Infra**| **Intent**| **Neighbor-Discovery**| **Registrar**| **Services**} {**aaa**| **all**| **database**| **events**| **ntp**| **packets**} {**info**| **moderate**| **severe**}

no debug autonomic{**Bootstrap**| **Channel-Discovery**| **Infra**| **Intent**| **Neighbor-Discovery**| **Registrar**| **Services**} {**aaa**| **all**| **database**| **events**| **ntp**| **packets**} {**info**| **moderate**| **severe**}

構文の説明

bootstrap	ブートストラップに関する情報のデバッグを有効にします。
Channel-Discovery	チャネル ディスカバリに関する情報のデバッグを有効にします。
Infra	インフラに関する情報のデバッグを有効にします。
Intent	目的に関する情報のデバッグを有効にします。
ネイバー探索	ネイバーに関する情報のデバッグを有効にします。
Registrar	レジストラに関する情報のデバッグを有効にします。
Services	自律型サービスに関する情報のデバッグを有効にします。
aaa	認証、認可、アカウンティングに関する情報のデバッグを有効にします。
all	すべてのデバッグを有効にします。
events	自律型イベントに関する情報を提供します。
ntp	Network Time Protocol（NTP）に関する情報のデバッグを有効にします。
パケット	自律型パケットに関する情報を提供します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

自律型ネットワークに関する情報をデバッグするには、このコマンドを使用します。

show autonomic control-plane

自律型コントロール プレーンに関する情報を表示するには、特権 EXEC モードで **show autonomic control-plane** コマンドを使用します。

show autonomic control-plane [**detail**]

構文の説明

detail	（任意）詳細情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

自律型コントロール プレーンに関する情報を表示するには、次のコマンドを使用します。

```
デバイス# show autonomic control-plane

VRF Name                        cisco_autonomic
Device Address                  FD08:2EEF:C2EE:0:E865:493B:ACFB:7
RPL                             floating-node, Dag-id = FD08:2EEF:C2EE:0:E865:493B:ACFB:5

Neighbor                           ACP            Channel ACP Security
-------------------------------------------------------------------------------
PID:WS-C3850-24U SN:FCW1934D05Z   Tunnel100002   DIKE
```

自律型コントロール プレーンに関する詳細情報を表示するには、次のコマンドを使用します。

```
デバイス# show autonomic control-plane detail

VRF Name                        cisco_autonomic
Device Address                  FD08:2EEF:C2EE:0:E865:493B:ACFB:7
```

```
RPL                              grounded-node, Dag-id = FD08:2EEF:C2EE:0:E865:493B:ACFB:1

Neighbor: PID:WS-C3850-24U SN:FCW1934D05Z
Uptime(Created Time): 00:12:16 ( 2016-07-15 05:38:53 UTC)
Supported ACP Channel: IPv6 GRE Tunnel
Negotiated ACP Channel: IPv6 GRE Tunnel
Tunnel Name Tunnel100000
Tunnel Source Interface ANI1
Tunnel Source FE80::5AAC:78FF:FE09:F383
Tunnel Destination FE80::3A20:56FF:FEF3:7158
Supported ACP Security: IPSec, DIKE
Negotiated ACP Security: DIKE
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *54*：*show autonomic control-plane* のフィールドの説明

フィールド	説明
VRF Name	VPN ルーティング/転送（VRF）名。
Device Address	IPv6 アドレス。
RPL	RPL ノードの詳細。
Neighbor	ネイバーの固有デバイス識別子（UDI）。
Tunnel Name	トンネル名。
Tunnel Source Interface	送信元トンネル インターフェイスの IP アドレス。
Tunnel Source	トンネルの送信元の IP アドレス。
Tunnel Destination	宛先の IP アドレス。

show autonomic device

自律型デバイス情報を表示するには、特権 EXEC モードで **show autonomic device** コマンドを使用します。

show autonomic device

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

自律型デバイス情報を表示するには、次のコマンドを使用します。

```
デバイス# show autonomic device

        Status                          Enabled
        Type                            Autonomic Node
        UDI                             PID:WS-C3650-24TD SN:FDO1942E1YK
        Device ID                       e865.493b.acfb-7
        Domain ID                       cisco.com
        Domain Certificate              (sub:) ou=cisco.com+serialNumber=PID:WS-C3650-24TD
SN:FDO1942E1YK,cn=e865.493b.acfb-7
        Certificate Serial Number       09
        Device Address                  FD08:2EEF:C2EE:0:E865:493B:ACFB:7
        Domain Cert is Valid
```

show autonomic interfaces

自律型インターフェイスに関する情報を表示するには、特権 EXEC モードで **show autonomic interfaces** コマンドを使用します。

show autonomic interfaces

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

自律型インターフェイスに関する情報を表示するには、次のコマンドを使用します。

```
デバイス# show autonomic interfaces

Interface                Channel Disc    AD Enabled      Intf Type
-------------------------------------------------------------------------------
GigabitEthernet0/0       None       No              L2 untagged If
GigabitEthernet1/0/1     None       No              L2 untagged If
GigabitEthernet1/0/2     None       No              L2 untagged If
GigabitEthernet1/0/3     Probing    No              L2 untagged If
```

```
GigabitEthernet1/0/4      None       No             L2 untagged If
GigabitEthernet1/0/5      None       No             L2 untagged If
GigabitEthernet1/0/6      None       No             L2 untagged If
GigabitEthernet1/0/7      None       No             L2 untagged If
GigabitEthernet1/0/8      None       No             L2 untagged If
GigabitEthernet1/0/9      None       No             L2 untagged If
GigabitEthernet1/0/10     None       No             L2 untagged If
GigabitEthernet1/0/11     None       No             L2 untagged If
GigabitEthernet1/0/12     None       No             L2 untagged If
GigabitEthernet1/0/13     None       No             L2 untagged If
GigabitEthernet1/0/14     None       No             L2 untagged If
GigabitEthernet1/0/15     None       No             L2 untagged If
GigabitEthernet1/0/16     None       No             L2 untagged If
GigabitEthernet1/0/17     None       No             L2 untagged If
GigabitEthernet1/0/18     None       No             L2 untagged If
GigabitEthernet1/0/19     None       No             L2 untagged If
GigabitEthernet1/0/20     None       No             L2 untagged If
GigabitEthernet1/0/21     None       No             L2 untagged If
GigabitEthernet1/0/22     None       No             L2 untagged If
GigabitEthernet1/0/23     None       No             L2 untagged If
GigabitEthernet1/0/24     None       No             L2 untagged If
GigabitEthernet1/1/1      None       No             L2 untagged If
GigabitEthernet1/1/2      None       No             L2 untagged If
TenGigabitEthernet1/1/3   None       No             L2 untagged If
TenGigabitEthernet1/1/4   None       No             L2 untagged If
Vlan1                     None       No             Virtual If
ANI1                      None       Yes            Virtual If
Loopback100000            None       No             Virtual If
Tunnel100002              None       No             Virtual If
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *55*：*show autonomic interface* のフィールドの説明

フィールド	説明
Interface	インターフェイス名。
Channel Disc	チャネル検出。
AD Enabled	

show autonomic intent

設定済みのインテント範囲を確認するには、特権 EXEC モードで **show autonomic intent** コマンドを使用します。

show autonomic intent

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

インテントは、自律型ドメイン内のすべてのノードに自動的に送信されます。そのため、すべてのノードで同じインテントが表示されます。

設定済みのインテント範囲に関する情報を表示するには、次のコマンドを使用します。

```
デバイス# show autonomic intent

Intent File : Available
Version Num : 1443520505 (Parsed)
Version Time: 2015-09-29 09:55:05 UTC
Outer Vlans : 30-35,40,45
Outer Vlans count : 8
```

show autonomic l2-channels

チャネル検出の結果を表示するには、特権 EXEC モードで **show autonomic l2-channels** コマンドを使用します。

show autonomic l2-channels

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

チャネル検出の結果を表示するには、次のコマンドを使用します。

```
デバイス# show autonomic l2-channels
```

```
AN L2 Channel Discovery Info :
Nbr UDI                          Encap    Our Intf   State   Retry
-------------------------------------------------------------------------------
PID:WS-C3850-24U SN:FCW1934D05Z  4018    Gi1/0/3      Active  1
```

詳細情報を表示するには、次のコマンドを使用します。

```
デバイス# show autonomic l2-channels detail

AN L2 Channel Discovery Info :
-------------------------------------------------------------------------------
Nbr UDI                : PID:WS-C3850-24U SN:FCW1934D05Z
ANI Intf               : ANI1
Encap                  : 0
Nbr Intf               : GigabitEthernet1/0/3
Our Intf               : GigabitEthernet1/0/3
Keepalives Missed      : 0
Channel Status         : Active
```

show autonomic service

自律型コントロール プレーン（ACP）を介してすべてのデバイスに配信されるサービス通知を確認するには、特権 EXEC モードで **show autonomic service** コマンドを使用します。

show autonomic service

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

サービスに関する情報を表示するには、次のコマンドを使用します。

```
デバイス# show autonomic service

       Service                 IP-Addr
       Syslog                  5000::100
       AAA                     5000::100
        AAA Accounting Port    1813
        AAA Authorization Port 1812
       Autonomic registrar     FD08:2EEF:C2EE:0:E865:493B:ACFB:1
        ANR type                IOS CA
       Config Server Address   5000::100
       Auto IP Server          UNKNOWN
```

show autonomic neighbor

自律型ネイバーに関する情報を表示するには、特権 EXEC モードで **show autonomic neighbor** コマンドを使用します。

show autonomic neighbor [**detail**]

構文の説明

detail	（任意）詳細情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、**show autonomic neighbor** コマンドの出力例を示します。

```
デバイス# show autonomic neighbor

UDI                                 Device-ID          Domain      Interface
------------------------------------------------------------------------------
PID:WS-C3850-24U  SN:FCW1934D05Z    e865.493b.acfb-5   cisco.com   ANI1
```

次に、**show autonomic neighbor detail** コマンドの出力例を示します。

```
デバイス# show autonomic neighbor detail

UDI: "PID:WS-C3850-24U SN:FCW1934D05Z"

       Device ID                     e865.493b.acfb-5
       Domain ID                     cisco.com
       Address                       FD08:2EEF:C2EE:0:E865:493B:ACFB:5
       State                         Nbr inside the Domain
       Credential                    Domain Cert
       Credential Validation         Passed
       Last Validated Time           2016-07-15 05:48:37 UTC
       Certificate Expiry Date       2017-07-15 05:30:39 UTC
       Certificate Expire Countdown  31534693 (secs)
       Number of Links connected     1

        Link:
            Local Interface:         ANI2
            Remote Interface:        ANI2
            IP Address:              FE80::3A20:56FF:FEF3:7158
            Uptime(Discovered Time):  00:14:21 ( 2016-07-15 05:38:05 UTC)
            Last Refreshed time:     0 seconds ago
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *56* : ***show autonomic neighbor detail*** のフィールドの説明

フィールド	説明
UDI	固有デバイス識別情報（UDI）。
Device Identifier	デバイス名。
Domain Identifier	ドメイン名。
State	ネイバーがドメインの内部にあるか、外部にあるかに関する情報。デバイスが自律型ドメイン内にある場合、有効なドメイン証明書が必要です。
Credential	検出方法。
Credential Validation	検出内容の検証。
Number of Links connected	検出されたネイバーの数。
Local Interface	ネイバーの接続元のインターフェイス。
Remote Interface	ネイバーの接続先のインターフェイス。
IP Address	ネイバーの IPv6 アドレス。

第 23 章

トレース コマンド

- トレースについて，1375 ページ
- set platform software trace，1378 ページ
- show platform software trace filter-binary，1382 ページ
- show platform software trace message，1383 ページ
- show platform software trace level，1387 ページ
- request platform software trace archive，1390 ページ
- request platform software trace rotate all，1391 ページ
- request platform software trace filter-binary，1392 ページ
- set platform software trace wireless switch active R0 hyperlocation，1393 ページ

トレースについて

トレースの概要

トレース機能により内部イベントが記録されます。トレース ファイルは自動的に作成され、crashinfo の下の tracelogs サブディレクトリに保存されます。

トレース ファイルのデータは、次の処理を行う場合に役立ちます。

- トラブルシューティング：スイッチに問題がある場合、トレース ファイルの出力により、問題の特定および解決に使用できる情報が得られる場合があります。
- デバッグ：トレース ファイルの出力は、システム動作の詳細情報を得るために役立ちます。

特定のモジュールに関する最新のトレース情報を表示するには、**show platform software trace message** コマンドを使用します。

トレース レベルを変更してトレース メッセージ出力の量を調整するために、**set platform software trace** コマンドを使用して新しいトレーシング レベルを設定できます。トレース レベルは、**set platform software trace** コマンドで **all-modules** キーワードを使用してプロセスごとに設定することも、プロセス内のモジュールごとに設定することもできます。

トレースログの場所

各プロセスは、btraceインフラストラクチャを使用してトレース メッセージをログに記録します。プロセスがアクティブのときは、対応するインメモリ トレースログが /tmp/<FRU>/trace/ ディレクトリにあります。ここで、<FRU> は、プロセスが実行されている場所（rp、fp、または cc）を表します。

トレースログ ファイルがプロセスに関して許可されている最大ファイル サイズの上限に達すると、またはプロセスが終了すると、次のディレクトリにローテーションされます。

- /crashinfo/tracelogs（スイッチで crashinfo: パーティションを使用できる場合）
- /harddisk/tracelogs（スイッチで crashinfo: パーティションを使用できない場合）

トレースログ ファイルは、ディレクトリに保存される前に圧縮されます。

トレースログの命名規則

btrace を使用して作成されるすべてのトレースログには、次の命名規則が適用されます。

<process_name>_<FRU><SLOT>-<BAY>.<pid>_<counter>.<creation_timestamp>.bin

ここで、counter は、64 ビットのフリーランニング カウンタで、当該プロセスの新しいファイルが作成されるたび増加します。たとえば、wcm_R0-0.1362_0.20151006171744.bin にようになります。圧縮されると、ファイル名に gz 拡張子が付加されます。

トレースログのサイズの上限およびローテーション ポリシー

トレースログ ファイルの最大サイズはプロセスごとに 1 MB で、保持されるトレースログ ファイルの最大数はプロセスごとに 25 です。

ローテーションおよびスロットリング ポリシー

最初は、すべての トレースログ ファイルが、初期ディレクトリの /tmp/<FRU>/trace から中継ディレクトリの /tmp/<FRU>/trace/stage に移されます。次に、btrace_rotate スクリプトによって、これらのトレースログが中継ディレクトリから /crashinfo/tracelogs ディレクトリに移されます。プロセスごとに /crashinfo/tracelogs ディレクトリに保存されるファイルの数が最大数の上限に達すると、そのプロセスの最も古いファイルが削除されますが、それより新しいファイルは保持されます。これは、最悪の場合、60 分ごとに繰り返されます。

その他、次の 2 種類のファイルセットが /crashinfo/tracelogs ディレクトリからパージされます。

- 標準命名規則を持たないファイル（fed_python.log などのいくつかの例外を除く）

- 2 週間以上保持されたファイル

エラーのあるプロセスがスイッチの機能に影響を与えないように、スロットリング ポリシーが導入されました。プロセスが非常に高い頻度でログを記録する（たとえば、そのプロセスに関して中継ディレクトリに 4 秒間隔で 17 以上のファイルが保存される）場合は常に、そのプロセスがスロットリングされます。そのプロセスのファイルは `/tmp/<FRU>/trace` から `/tmp/<FRU>/trace/stage` にローテーションされませんが、最大サイズに達すると削除されます。ファイル数が 7 以下になるとスロットリングが再度有効になります。

トレース レベル

トレース レベルは、トレース バッファまたはトレース ファイルに保存する必要のあるモジュール情報の量を決定します。

次の表に、使用可能なすべてのトレース レベルを示し、各トレース レベルで表示されるメッセージについて説明します。

表 *57*：トレース レベルとその内容

トレース レベル	説明
Emergency	システムが使用不能になる問題のメッセージです。
Error	システム エラーについてのメッセージです。
Warning	システム警告についてのメッセージです。
Notice	重大な問題に関するメッセージです。ただし、スイッチは通常どおり動作しています。
Informational	単に情報を提供するだけのメッセージです。
Debug	デバッグレベルの出力を提供するメッセージです。
Verbose	生成可能なすべてのトレース メッセージが送信されます。
Noise	モジュールについての生成可能なすべてのトレース メッセージが記録されます。 ノイズ レベルは常に最上位のトレース レベルに相当します。今後、トレース機能の拡張が行われ、さらに低いトレース レベルが導入された場合でも、ノイズ レベルはこの新しい拡張機能のレベルと同じレベルに相当します。

set platform software trace

プロセス内の特定のモジュールのトレース レベルを設定するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software trace** コマンドを使用します。

set platform software trace *process slot module trace-level*

構文の説明

process	トレース レベルが設定されているプロセス。次のオプションがあります。 • **chassis-manager**：シャーシマネージャ プロセス。 • **cli-agent**：CLI エージェント プロセス。 • **dbm**：データベース マネージャ プロセス。 • **emd**：環境モニタリング プロセス。 • **fed**：フォワーディング エンジン ドライバ プロセス。 • **forwarding-manager**：フォワーディング マネージャ プロセス。 • **host-manager**：ホスト マネージャ プロセス。 • **iomd**：入出力モジュール デーモン（IOMd）プロセス。 • **ios**：IOS プロセス。 • **license-manager**：ライセンス マネージャ プロセス。 • **logger**：ロギング マネージャ プロセス。 • **platform-mgr**：プラットフォーム マネージャ プロセス。 • **pluggable-services**：プラグ可能サービス プロセス。 • **replication-mgr**：レプリケーション マネージャ プロセス。 • **shell-manager**：シェル マネージャ プロセス。 • **smd**：セッション マネージャ プロセス。 • **table-manager**：テーブル マネージャ サーバ。 • **wireless**：ワイヤレス コントローラ モジュール プロセス。 • **wireshark**：Embedded Packet Capture（EPC; 組み込みパケット キャプチャ）Wireshark プロセス。

slot	トレース レベルが設定されているプロセスが、稼働しているハードウェア スロット。次のオプションがあります。 • *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロット番号。たとえば、スイッチの SIP スロット 2 に SIP を指定するには、2 を入力します。 • *SIP-slot*/*SPA-bay*：SIP スイッチのスロット番号とその SIP の共有ポート アダプタ（SPA）ベイの番号。たとえば、スイッチのスロット 3 に SIP を指定し、その SIP のベイ 2 に SPA を指定するには、3/2 を入力します。 • **F0**：スロット 0 の組み込みサービス プロセッサ。 • **FP active**：アクティブな組み込みサービス プロセッサ。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。 • **switch**<*number*>：指定された番号のスイッチ。 • **switch active**：アクティブ スイッチ。 • **switch standby**：スタンバイ スイッチ。
module	トレース レベルが設定されているプロセス内のモジュール。

trace-level	トレース レベルです。次のオプションがあります。 • **debug**：デバッグ レベルのトレース。デバッグレベルのトレース メッセージは、モジュールに関する大量の詳細を提供する緊急でないメッセージです。 • **emergency**：緊急レベルのトレース。緊急レベルのトレース メッセージは、システムが使用不能であることを示すメッセージです。 • **error**：エラー レベルのトレース。エラーレベルのトレース メッセージは、システム エラーを示すメッセージです。 • **info**：情報レベルのトレース。情報レベルのトレース メッセージは、システムに関する情報を提供する緊急でないメッセージです。 • **noise**：ノイズ レベルのトレース。ノイズ レベルは、常に可能なトレース レベルの中の最高レベルに相当し、考えられるすべてのトレース メッセージを生成します。 ノイズ レベルは、モジュールに関して可能な最高レベルのトレース メッセージに相当します。これは、このコマンドの将来の拡張で、ユーザが寄り高いトレース レベルを設定できるオプションが追加された場合にも、当てはまります。 • **notice**：重大な問題に関するメッセージです。ただし、スイッチは通常どおり動作しています。 • **verbose**：デバッグ レベルのトレース。トレース レベルが verbose に設定されている場合は、考えられるすべてのトレース メッセージが送信されます。 • **warning**：警告メッセージ。

コマンド デフォルト

すべてのモジュールのデフォルトのトレース レベルは **notice** です。

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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

module オプションは、プロセスおよび *hardware-module* によって異なります。このコマンドを入力する際に、各キーワード シーケンスで使用可能な *module* オプションを確認するには、? オプションを使用します。

トレース メッセージを表示するには、**show platform software trace message** コマンドを使用します。

トレース ファイルは、harddisk: ファイル システムのトレース ログ ディレクトリに保存されます。これらのファイルは、スイッチの動作に影響を与えずに削除できます。

トレース ファイル出力は、デバッグに使用されます。トレース レベルは、モジュールに関するどのぐらいの量の情報をトレース ファイルに保存するかを決定する設定です。

例

次に、dbm プロセスのすべてのモジュールのトレース レベルを設定する例を示します。

```
Device# set platform software trace dbm R0 all-modules debug
```

show platform software trace filter-binary

特定のモジュールの最新のトレース情報を表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show platform software trace filter-binary** コマンドを使用します。

show platform software trace filter-binary*modules* [**context** *mac-address*]

構文の説明

context*mac-address*	フィルタ処理に使用されるコンテキストを表します。また、モジュール名とトレース レベルに基づいてフィルタ処理できます。コンテキスト キーワードは、タグが付いているトレースに基づき MAC アドレスまたは他の引数を受け入れます。

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
Cisco IOS XE Denali 16.1.1	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、モジュールに関連するすべてのプロセス全体で /tmp/.../ に存在するすべてのログを照合してソートします。指定されたモジュールに関連するすべてのプロセスのトレースログがコンソールに出力されます。このコマンドでは、同じコンテンツのcollated_log_{system time} という名前のファイルも /crashinfo/tracelogs ディレクトリに生成されます。

例

次に、ワイヤレス モジュールのトレース情報を表示する例を示します。

```
Device# show platform software trace filter-binary wireless
```

show platform software trace message

プロセスのトレース メッセージを表示するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software trace** コマンドを使用します。

show platform software trace message *process slot*

構文の説明

process	設定されているトレース レベル。次のオプションがあります。 • **chassis-manager**：Chassis Manager プロセス。 • **cli-agent**：CLI Agent プロセス。 • **cmm**：CMM プロセス。 • **dbm**：Database Manager プロセス。 • **emd**：Environmental Monitoring プロセス。 • **fed**：Forwarding Engine Driver プロセス。 • **forwarding-manager**：Forwarding Manager プロセス。 • **geo**：Geo Manager プロセス。 • **host-manager**：Host Manager プロセス。 • **interface-manager**：Interface Manager プロセス。 • **iomd**：Input/Output Module daemon（IOMd）プロセス。 • **IOS**：IOS プロセス。 • **license-manager**：License Manager プロセス。 • **logger**：Logging Manager プロセス。 • **platform-mgr**：Platform Manager プロセス。 • **pluggable-services**：Pluggable Services プロセス。 • **replication-mgr**：Replication Manager プロセス。 • **shell-manager**：Shell Manager プロセス。 • **sif**：Stack Interface（SIF）Manager プロセス。 • **smd**：Session Manager プロセス。 • **stack-mgr**：Stack Manager プロセス。 • **table-manager**：Table Manager Server。 • **thread-test**：Multithread Manager プロセス。 • **virt-manager**：Virtualization Manager プロセス。 • **wireless**：ワイヤレス コントローラ モジュール プロセス。

slot

トレース レベルが設定されているプロセスを実行中のハードウェア スロット。次のオプションがあります。

- *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
- *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
- **F0**：Embedded Service Processor スロット 0。
- **FP active**：アクティブな Embedded Service Processor。
- **R0**：スロット 0 のルート プロセッサ。
- **RP active**：アクティブなルート プロセッサ。
- **switch**<*number*>：スイッチおよび指定された番号。
- **switch active**：アクティブ スイッチ。
- **switch standby**：スタンバイ スイッチ。
  - *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
  - *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
  - **F0**：スロット 0 の Embedded Service Processor。
  - **FP active**：アクティブな Embedded Service Processor。
  - **R0**：スロット 0 のルート プロセッサ。
  - **RP active**：アクティブなルート プロセッサ。

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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、Stack Manager プロセスおよび Forwarding Engine Driver プロセスのトレース メッセージを表示する例を示します。

```
Device# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect

Device# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Single message size is greater
 than 1024
11/02 10:55:01.822 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered module
 [88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered module
 [89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]:  UUID: 0, ra: 0 (note): Pending connection to server
10.129.1.0
11/01 09:53:34.227 [xcvr]: [18846]:  UUID: 0, ra: 0 (ERR): FRU hardware authentication Fail,
 result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C receive
 failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
```

show platform software trace level

特定のプロセスですべてのモジュールのトレース レベルを表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show platform software trace level** コマンドを使用します。

show platform software trace level *process slot*

構文の説明

process	トレース レベルが設定されているプロセス。次のオプションがあります。 • **chassis-manager**：Chassis Manager プロセス。 • **cli-agent**：CLI Agent プロセス。 • **cmm**：CMM プロセス。 • **dbm**：Database Manager プロセス。 • **emd**：Environmental Monitoring プロセス。 • **fed**：Forwarding Engine Driver プロセス。 • **forwarding-manager**：Forwarding Manager プロセス。 • **geo**：Geo Manager プロセス。 • **host-manager**：Host Manager プロセス。 • **interface-manager**：Interface Manager プロセス。 • **iomd**：Input/Output Module daemon（IOMd）プロセス。 • **IOS**：IOS プロセス。 • **license-manager**：License Manager プロセス。 • **logger**：Logging Manager プロセス。 • **platform-mgr**：Platform Manager プロセス。 • **pluggable-services**：Pluggable Services プロセス。 • **replication-mgr**：Replication Manager プロセス。 • **shell-manager**：Shell Manager プロセス。 • **sif**：Stack Interface（SIF）Manager プロセス。 • **smd**：Session Manager プロセス。 • **stack-mgr**：Stack Manager プロセス。 • **table-manager**：Table Manager Server。 • **thread-test**：Multithread Manager プロセス。 • **virt-manager**：Virtualization Manager プロセス。 • **wireless**：ワイヤレス コントローラ モジュール プロセス。

slot	トレース レベルが設定されているプロセスを実行中のハードウェア スロット。次のオプションがあります。 • *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 • *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 • **F0**：スロット 0 の Embedded Service Processor。 • **F1**：スロット 1 の Embedded Service Processor。 • **FP active**：アクティブな Embedded Service Processor。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。 • **switch**<*number*>：スイッチおよび指定された番号。 • **switch active**：アクティブ スイッチ。 • **switch standby**：スタンバイ スイッチ。 ◦ *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 ◦ *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 ◦ **F0**：スロット 0 の Embedded Service Processor。 ◦ **FP active**：アクティブな Embedded Service Processor。 ◦ **R0**：スロット 0 のルート プロセッサ。 ◦ **RP active**：アクティブなルート プロセッサ。

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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、トレース レベルを表示する例を示します。

```
Device# show platform software trace level dbm switch active R0
Module Name                      Trace Level
----------------------------------------------------
binos                            Notice
binos/brand                      Notice
bipc                             Notice
btrace                           Notice
bump_ptr_alloc                   Notice
cdllib                           Notice
chasfs                           Notice
dbal                             Informational
dbm                              Debug
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
green-be                         Notice
ios-avl                          Notice
klib                             Debug
services                         Notice
sw_wdog                          Notice
syshw                            Notice
tdl_cdlcore_message              Notice
tdl_dbal_root_message            Notice
tdl_dbal_root_type               Notice
```

request platform software trace archive

スイッチでの最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレース ログをアーカイブし、これを指定された場所に保存するには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace archive** コマンドを使用します。

request platform software trace archive [**last** *number-of-days* [**days** [**target** *location*]] | **target** *location*]

構文の説明

last *number-of-days*	トレース ファイルをアーカイブする必要がある日数を指定します。
target *location*	アーカイブ ファイルの場所と名前を指定します。

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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このアーカイブ ファイルは、tftp コマンドまたは scp コマンドを使用してシステムからコピーできます。

例

次に、過去 5 日以降にスイッチで実行されているプロセスのすべてのトレース ログをアーカイブする例を示します。

```
Device# request platform software trace archive last 5 days target flash:test_archive
```

request platform software trace rotate all

現在のインメモリ トレース ログを crashinfo パーティションに循環させ、プロセスごとの新しいインメモリ トレースログを開始するには、特権EXECモードまたはユーザEXECモードで**request platform software trace rotate all** コマンドを使用します。

request platform software trace rotate all

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
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

トレースログファイルは読み取り専用を目的としています。ファイルの内容は編集しないでください。特定のログ セットを表示するために、ファイルの内容を削除する必要がある場合は、このコマンドを使用して新しいトレース ログ ファイルを開始します。

例

次に、過去1日以降にスイッチで実行されているプロセスのすべてのインメモリ トレース ログを循環させる例を示します。

```
Device# request platform software trace slot switch active R0 archive last 1 days target
flash:test
```

request platform software trace filter-binary

トレースログサブディレクトリに存在するすべてのアーカイブログを照合して並べ替えるには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace filter-binary** コマンドを使用します。

request platform software trace filter-binary *modules* [**context** *mac-address*]

構文の説明

context *mac-address*	フィルタ処理するために使用されるコンテキストを表します。また、モジュール名とトレース レベルに基づいてフィルタ処理することもできます。contextキーワードは、タグ付けされたトレースに基づいて、MAC アドレスまたはその他の引数のいずれかを受け入れます。

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
Cisco IOS XE Denali 16.1.1	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、モジュールに関連するすべてのプロセスを対象に、トレースログ サブディレクトリに存在するすべてのアーカイブされたログを照合して並べ替えます。さらに、このコマンドは同じ内容の `collated_log_{system time}` という名前のファイルを `/crashinfo/tracelogs` ディレクトリに生成します。

例

次に、ワイヤレス モジュールのトレース情報を表示する例を示します。

```
Device# request platform software trace filter-binary wireless
```

set platform software trace wireless switch active R0 hyperlocation

Cisco Hyperlocation 関連のメッセージをトレースするには、**set platform software trace wireless switch active R0 hyperlocation** コマンドを使用します。

set platform software trace wireless switch active R0 hyperlocation {**debug** | **emergency** | **error** | **info** | **noise** | **notice** | **verbose** | **warning**}

構文の説明

debug	デバッグ メッセージ
emergency	緊急事態が考えられるメッセージ
error	エラー メッセージ
info	通知メッセージ
noise	考えられる最大のメッセージ
notice	通知メッセージ
verbose	詳細デバッグ メッセージ
warning	警告メッセージ

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

第 XX 部

VideoStream

- VideoStream コマンド, 1397 ページ

第 24 章

VideoStream コマンド

- ap dot11 media-stream multicast-direct, 1397 ページ
- show ap dot11, 1398 ページ
- show wireless media-stream group, 1399 ページ
- wireless media-stream multicast-direct, 1400 ページ
- wireless media-stream, 1401 ページ

ap dot11 media-stream multicast-direct

2.4 GHz/5 GHz 帯域のマルチキャスト ダイレクトを設定するには、**apdot11media-streammulticast-direct** コマンドを使用します。

ap dot11 {**24ghz**| **5ghz**} **media-stream** {**multicast-direct** {**admission-besteffort**| **client-maximum** *value*| **radio-maximum** *value*}| **video-redirect**}

構文の説明

multicast-direct	802.11 帯域のマルチキャスト ダイレクトを設定します。
admission-besteffort	ベスト エフォート キューにメディア ストリームを許可します。
client-maximum*value*	クライアントで許可されるストリームの最大数を指定します。
radio-maximum*value*	2.4 GHz または 5 GHz 帯域で許可されるストリームの最大数を指定します。
video-redirect	非マルチキャスト ダイレクト ビデオを無線で BestEffort キューにリダイレクトします。

コマンド デフォルト

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

802.11 ネットワークのメディア ストリーム マルチキャスト ダイレクト パラメータを設定する前に、ネットワークが非動作であることを確認します。

例

次に、2.4 GHz 帯域のマルチキャスト ダイレクトを設定する例を示します。

```
(Cisco Controller) >Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 24ghz media-stream multicast-direct
```

関連トピック

wireless media-stream multicast-direct, （1400 ページ）

show ap dot11

802.11 帯域パラメータを表示するには、**showapdot11** コマンドを使用します。

show ap dot11 {**24ghz**| **5ghz**} {**media-stream rrc**| **network**| **profile**| **summary**}

構文の説明

media-streamrrc	メディア ストリーム設定を表示します。
network	ネットワーク設定を表示します。
profile	すべての Cisco AP のプロファイル情報を表示します。
summary	802.11b および 802.11a Cisco AP の設定と統計情報を表示します。

コマンド デフォルト

なし ザ EXEC コマンド モードまたは特権 EXEC コマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

なし。

次に、**show ap dot11 24ghz media-stream rrc** コマンドの出力例を示します。

```
Device#show ap dot11 24ghz media-stream rrc

Multicast-direct                : Disabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio      : Auto
Max Allowed Streams Per Client     : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

関連トピック

wireless media-stream, （1401 ページ）

show wireless media-stream group

ワイヤレス メディア ストリーム グループ情報を表示するには、**show wireless media-stream group** コマンドを使用します。

show wireless media-stream group {**detail** *groupName*| **summary**}

構文の説明

detail*groupName*	コマンドで指定されているグループのメディア ストリーム グループの設定の詳細を表示します。
summary	メディア ストリーム グループの設定の概要を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC モードまたは特権 EXEC モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

なし。

次に、**show wireless media-stream group detail GRP1** コマンドの出力例を示します。

```
Device#show wireless media-stream group detail GRP1
```

関連トピック

wireless media-stream, （1401 ページ）

wireless media-stream multicast-direct

マルチキャストダイレクトのステータスを設定するには**media-streammulticast-direct** コマンドを使用します。マルチキャストダイレクトのステータスを削除するには、このコマンドのno形式を使用します。

no wireless media-stream multicast-direct

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。WLAN Quality of Service（QoS）を gold または platinum のいずれかに設定する必要があります。

例

次に、ワイヤレス LAN メディア ストリームのマルチキャストダイレクトを設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless media-stream multicast-direct
```

wireless media-stream

さまざまなパラメータを設定するには、**wirelessmedia-stream** コマンドを使用します。

wireless media-stream group *groupName* [*startipAddr endipAddr*]

wireless media-stream group{avg-packet-size default exit max-bandwidth no policy qos}

wireless media-stream {**multicast-direct**| **message** [**phone** *phone*| **URL** *URL*| **Notes** *Notes*| **Email** *Email*]}

構文の説明

group*groupName*	グループのマルチキャスト ダイレクト ステータスを設定します。
startipAddr	グループの開始 IP アドレスを設定します。
endipAddr	グループの終了 IP アドレスを設定します。

group*avg-packet-size*	平均パケット サイズを設定します。
group*default*	コマンドをデフォルト値に設定します。
group *exit*	サブモードを終了します。
group*max-bandwidth*	予想されるストリームの最大帯域幅を Kbps 単位で設定します。
group *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。
group*policy*	メディア ストリームのアドミッション ポリシーを設定します。
group *qos*	エア QoS クラスを <'video'> ONLY に設定します。
multicast-direct	マルチキャスト ダイレクト ステータスを設定します。
message	セッション アナウンス メッセージを設定します。
phone*phone*	セッション アナウンスの電話番号を設定します。
URL*URL*	セッション アナウンス URL を設定します。
Notes*Notes*	セッション アナウンス メモを設定します。
Email*Email*	セッション アナウンス電子メールを設定します。

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

例

次に、予想されるマルチキャスト宛先アドレス、ストリームの帯域幅の使用量およびストリームの優先順位のパラメータなど、各メディア ストリームとそのパラメータを設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless media-stream group GROUP1 231.1.1.1 231.1.1.10
```

第 XXI 部

VLAN

- VLAN コマンド，1407 ページ

第 25 章

VLAN コマンド

- client vlan, 1408 ページ
- clear vtp counters, 1409 ページ
- debug platform vlan, 1409 ページ
- debug sw-vlan, 1410 ページ
- debug sw-vlan ifs, 1412 ページ
- debug sw-vlan notification, 1413 ページ
- debug sw-vlan vtp, 1415 ページ
- interface vlan, 1416 ページ
- show platform vlan, 1418 ページ
- show vlan, 1419 ページ
- show vtp, 1422 ページ
- show wireless vlan group, 1429 ページ
- switchport priority extend, 1430 ページ
- switchport trunk, 1431 ページ
- vlan, 1434 ページ
- vlan dot1q tag native, 1441 ページ
- vtp（グローバル コンフィギュレーション）, 1442 ページ
- vtp（インターフェイス コンフィギュレーション）, 1448 ページ
- vtp primary, 1449 ページ
- wireless broadcast vlan, 1450 ページ

client vlan

WLAN インターフェイスまたはインターフェイス グループを設定するには、**clientvlan** コマンドを使用します。WLAN インターフェイ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。

client vlan *interface-id-name-or-group-name*

no client vlan

構文の説明

interface-id-name-or-group-name	インターフェイス ID、名前、または VLAN グループ名。インターフェイス ID は、複数桁で指定することもできます。

コマンド デフォルト

デフォルト インターフェイスが設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント VLAN をイネーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client vlan client-vlan1
Device(config-wlan)# end
```

次に、WLAN 上のクライアント VLAN をディセーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no client vlan
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

clear vtp counters

VLAN Trunking Protocol（VTP）およびプルーニング カウンタをクリアするには、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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次の例では、VTP カウンタをクリアする方法を示します。

```
Device# clear vtp counters
```

情報が削除されたことを確認するには、**show vtp counters** 特権 EXEC コマンドを入力します。

関連トピック

show vtp, （1422 ページ）

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、特権 EXEC モードで **debug platform 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には、このコマンドの **no** 形式を使用します。

debug platform vlan [**error**| **event**] [**switch** *switch-number*]

no debug platform vlan [**error**| **event**] [**switch** *switch-number*]

構文の説明

error	（任意）VLAN エラー デバッグ メッセージを表示します。
event	（任意）VLAN 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。
switch *switch-number*	（任意）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スタック メンバ番号を指定します。 このキーワードは、スタック対応スイッチでのみサポートされています。

コマンド 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
Cisco IOS XE 3.2SE	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 platform vlan コマンドは、**no debug platform vlan** コマンドと同じです。

次の例では、VLAN エラー デバッグ メッセージを表示する方法を示します。

```
Device# debug platform vlan error
```

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には、このコマンドの **no** 形式を使用します。

debug sw-vlan {**badpmcookies**| **cfg-vlan** {**bootup**| **cli**}| **events**| **ifs**| **management**| **mapping**| **notification**| **packets**| **redundancy**| **registries**| **vtp**}

no debug sw-vlan {badpmcookies| cfg-vlan {bootup| cli}| events| ifs| management| mapping| notification| packets| redundancy| registries| vtp}

構文の説明

badpmcookies	不良ポート マネージャ クッキーの VLAN マネージャ インシデントに関するデバッグ メッセージを表示します。
cfg-vlan	VLAN 設定デバッグ メッセージを表示します。
bootup	スイッチが起動すると、メッセージが表示されます。
cli	コマンドライン インターフェイス（CLI）が VLAN コンフィギュレーション モードである場合のメッセージを表示します。
events	VLAN マネージャ イベントのデバッグ メッセージを表示します。
ifs	VLAN マネージャ IOS ファイル システム（IFS）のデバッグ メッセージを表示します。詳細については、「debug sw-vlan ifs, （1412 ページ）」を参照してください。
management	内部 VLAN の VLAN マネージャ管理のデバッグ メッセージを表示します。
mapping	VLAN マッピングのデバッグ メッセージを表示します。
notification	VLAN マネージャ通知のデバッグ メッセージを表示します。詳細については、「debug sw-vlan notification, （1413 ページ）」を参照してください。
packets	パケット処理およびカプセル化プロセスのデバッグ メッセージを表示します。
redundancy	VTP VLAN 冗長性のデバッグ メッセージを表示します。
registries	VLAN マネージャ レジストリのデバッグ メッセージを表示します。
vtp	VLAN Trunking Protocol（VTP）コードのデバッグ メッセージを表示します。詳細については、「debug sw-vlan vtp, （1415 ページ）」を参照してください。

コマンド 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
Cisco IOS XE 3.2SE	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 sw-vlan コマンドは、**no debug sw-vlan** コマンドと同じです。

スイッチ スタック上でデバッグをイネーブルにした場合、アクティブ スイッチ でのみイネーブルになります。特定のスタック メンバをデバッグする場合は、**session switch***stack-member-number* 特権 EXEC コマンドを使用してアクティブ スイッチから CLI セッションを開始できます。

次に、VLAN マネージャ イベントのデバッグ メッセージを表示する例を示します。

```
Device# debug sw-vlan events
```

関連トピック

- debug sw-vlan ifs, （1412 ページ）
- debug sw-vlan notification, （1413 ページ）
- debug sw-vlan vtp, （1415 ページ）
- show vlan, （1419 ページ）
- show vtp, （1422 ページ）

debug sw-vlan ifs

VLAN マネージャ IOS File System（IFS）エラーテストのデバッグをイネーブルにするには、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には、このコマンドの **no** 形式を使用します。

debug sw-vlan ifs {**open** {**read**| **write**}| **read** {**1**| **2**| **3**| **4**}| **write**}

no debug sw-vlan ifs {**open** {**read**| **write**}| **read** {**1**| **2**| **3**| **4**}| **write**}

構文の説明

open read	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。
open write	VLAN マネージャ IFS 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。

read	指定されたエラーテスト（**1**、**2**、**3**、または**4**）に関するファイル読み取り動作のデバッグ メッセージを表示します。
write	ファイル書き込み動作のデバッグ メッセージを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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 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。

スイッチ スタック上でデバッグをイネーブルにした場合、アクティブ スイッチ でのみイネーブルになります。特定のスタック メンバをデバッグする場合は、**session switch***stack-member-number* 特権 EXEC コマンドを使用してアクティブ スイッチから CLI セッションを開始できます。

次の例では、ファイル書き込み動作のデバッグ メッセージを表示する方法を示します。

```
Device# debug sw-vlan ifs write
```

関連トピック

show vlan, （1419 ページ）

debug sw-vlan notification

VLAN マネージャ通知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には、このコマンドの **no** 形式を使用します。

debug sw-vlan notification {**accfwdchange**| **allowedvlancfgchange**| **fwdchange**| **linkchange**| **modechange**| **pruningcfgchange**| **statechange**}

no debug sw-vlan notification {**accfwdchange**| **allowedvlancfgchange**| **fwdchange**| **linkchange**| **modechange**| **pruningcfgchange**| **statechange**}

構文の説明

accfwdchange	集約アクセス インターフェイス スパニングツリー転送変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
allowedvlancfgchange	許可VLANの設定変更に関するVLANマネージャ通知のデバッグ メッセージを表示します。
fwdchange	スパニングツリー転送変更に関するVLANマネージャ通知のデバッグ メッセージを表示します。
linkchange	インターフェイス リンクステート変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
modechange	インターフェイスモード変更のVLANマネージャ通知のデバッグ メッセージを表示します。
pruningcfgchange	プルーニング設定変更のVLANマネージャ通知のデバッグ メッセージを表示します。
statechange	インターフェイス ステート変更の VLAN マネージャ通知のデバッグ メッセージを表示します。

コマンド 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
Cisco IOS XE 3.2SE	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 sw-vlan notification コマンドは、**no debug sw-vlan notification** コマンドと同じです。

スイッチ スタック上でデバッグをイネーブルにした場合、アクティブ スイッチ でのみイネーブルになります。特定のスタック メンバをデバッグする場合は、**session switch** *stack-member-number* 特権 EXEC コマンドを使用してアクティブ スイッチから CLI セッションを開始できます。

次に、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 メッセージを表示する例を示します。

```
Device# debug sw-vlan notification
```

関連トピック

show vlan, （1419 ページ）

debug sw-vlan vtp

VLAN Trunking Protocol（VTP）コードのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan vtp** コマンドを使用します。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 sw-vlan vtp {**events**| **packets**| **pruning** [**packets**| **xmit**]| **redundancy**| **xmit**}

no debug sw-vlan vtp {**events**| **packets**| **pruning**| **redundancy**| **xmit**}

構文の説明

events	汎用の論理フローのデバッグ メッセージおよび VTP コード内の VTP_LOG_RUNTIME マクロによって生成された VTP メッセージの詳細を表示します。
packets	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。
pruning	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。
packets	（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。
xmit	（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。
redundancy	VTP 冗長性のデバッグ メッセージを表示します。

xmit	VTP コードが 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。

コマンド 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
Cisco IOS XE 3.2SE	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 sw-vlan vtp コマンドは、**no debug sw-vlan vtp** コマンドと同じです。

pruning キーワードの後に追加のパラメータを入力しない場合は、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。

スイッチ スタック上でデバッグをイネーブルにした場合、アクティブ スイッチ でのみイネーブルになります。特定のスタック メンバをデバッグする場合は、**session switch***stack-member-number* 特権 EXEC コマンドを使用してアクティブ スイッチから CLI セッションを開始できます。

次に、VTP 冗長性のデバッグ メッセージを表示する例を示します。

```
Device# debug sw-vlan vtp redundancy
```

関連トピック

show vtp, （1422 ページ）

interface vlan

ダイナミック スイッチ仮想インターフェイス（SVI）を作成するか、既存のダイナミック SVI にアクセスし、インターフェイス コンフィギュレーション モードを開始するには、グローバル コ

ンフィギュレーション モードで **interface vlan** コマンドを使用します。SVI を削除するには、このコマンドの **no** 形式を使用します。

interface vlan *vlan-id*

no interface vlan *vlan-id*

構文の説明

vlan-id	VLAN 番号。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

デフォルトの VLAN インターフェイスは VLAN 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

SVI は、特定の VLAN に対して最初に **interface vlan** *vlan-id* コマンドを入力したときに作成されます。*vlan-id* は、IEEE 802.1Q カプセル化トランク上のデータ フレームに対応する VLAN タグ、またはアクセス ポート用に設定された VLAN ID に対応します。

（注） 物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

no interface vlan *vlan-id* コマンドを使用して削除した SVI は、**show interfaces** 特権 EXEC コマンドの出力に表示されなくなります。

（注） VLAN 1 インターフェイスを削除することはできません。

削除されたインターフェイスに対して **interface vlan** *vlan-id* コマンドを入力すると、削除された SVI を元に戻すことができます。インターフェイスはバックアップとなりますが、それまでの設定は削除されます。

スイッチまたはスイッチ スタック上で設定された SVI の数と、設定された他の機能の数の相互関係によっては、ハードウェア制限により、CPU 使用率に影響が出る可能性があります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用して、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。

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

次の例では、VLAN ID 23 の新しい SVI を作成し、インターフェイス コンフィギュレーション モードを開始する方法を示します。

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

関連トピック

show interfaces, （205 ページ）

show platform vlan

プラットフォーム依存 VLAN 情報を表示するには、**show platform vlan** 特権 EXEC コマンドを使用します。

show platform vlan [*vlan-id*] [**switch** *switch-number*]

構文の説明

vlan-id	（任意）VLAN の ID。指定できる範囲は 1 ～ 4094 です。
switch *switch-number*	（任意）指定されたスタック メンバの VLAN のみを表示します。

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
Cisco IOS XE 3.2SE	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。

次の例では、プラットフォーム依存 VLAN 情報を表示する方法を示します。

```
Device# show platform vlan
```

show vlan

設定されたすべての VLAN またはスイッチ上の VLAN（VLAN ID または名前を指定した場合）のパラメータを表示するには、特権 EXEC モードで **show vlan** コマンドを使用します。

show vlan [**brief**| **dot1q tag native**| **group**| **id** *vlan-id*| **mtu**| **name** *vlan-name*| **remote-span**| **summary**]

構文の説明

brief	（任意）VLAN ごとに VLAN 名、ステータス、およびポートを 1 行で表示します。
dot1q tag native	（任意）IEEE 802.1Q ネイティブ VLAN タギング ステータスを表示します。
group	（任意VLAN グループについての情報を表示します。
id *vlan-id*	（任意）VLAN ID 番号で特定された 1 つの VLAN に関する情報を表示します。*vlan-id* に指定できる範囲は 1 ～ 4094 です。
mtu	（任意）VLAN のリストと、VLAN のポートに設定されている最小および最大伝送単位（MTU）サイズを表示します。
name *vlan-name*	（任意）VLAN 名で特定された 1 つの VLAN に関する情報を表示します。VLAN 名は、1 ～ 32 文字の ASCII 文字列です。
remote-span	（任意）Remote SPAN（RSPAN）VLAN に関する情報を表示します。
summary	（任意）VLAN サマリー情報を表示します。

（注） **ifindex** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

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
Cisco IOS XE 3.2SE	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 と MaxMTU を持つポート名が表示されます。

次の例では、**show vlan** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24, Gi1/0/25
                                                Gi1/0/26, Gi1/0/27, Gi1/0/28
                                                Gi1/0/29, Gi1/0/30, Gi1/0/31
                                                Gi1/0/32, Gi1/0/33, Gi1/0/34
                                                Gi1/0/35, Gi1/0/36, Gi1/0/37
                                                Gi1/0/38, Gi1/0/39, Gi1/0/40
                                                Gi1/0/41, Gi1/0/42, Gi1/0/43
                                                Gi1/0/44, Gi1/0/45, Gi1/0/46
                                                Gi1/0/47, Gi1/0/48
2    VLAN0002                         active
40   vlan-40                          active
300  VLAN0300                         active
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
40   enet  100040     1500  -      -      -        -    -        0      0
300  enet  100300     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
2000 enet  102000     1500  -      -      -        -    -        0      0
3000 enet  103000     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
2000,3000

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

表 *58*：*show vlan* コマンドの出力フィールド

フィールド	説明
VLAN	VLAN 番号。
Name	VLAN の名前（設定されている場合）。
Status	VLAN のステータス（active または suspend）。
Ports	VLAN に属するポート。
Type	VLAN のメディア タイプ。
SAID	VLAN のセキュリティ アソシエーション ID 値。
MTU	VLAN の最大伝送単位サイズ。
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。

フィールド	説明
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 dot1q tag native** コマンドの出力を示します。

```
Device> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

次の例では、**show vlan summary** コマンドの出力を示します。

```
Device> 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。

```
Device# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi1/0/7, Gi1/0/8
2    VLAN0200                         active    Gi2/0/1, Gi2/0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
Disabled
```

関連トピック

switchport mode

vlan, （1434 ページ）

show vtp

VLAN Trunking Protocol（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

counters	デバイスの VTP 統計情報を表示します。
devices	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。このキーワードは、デバイスが VTP バージョン 3 を実行していない場合だけ適用されます。

conflicts	（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。デバイスが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。
interface	すべてのインターフェイスまたは指定されたインターフェイスに対するVTP のステータスおよび設定を表示します。
interface-id	（任意）VTPステータスおよび設定を表示するインターフェイス。ここ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。
password	設定されたVTPパスワードを表示します（特権EXECモードでのみ使用可能）。
status	VTP 管理ドメインのステータスに関する一般情報を表示します。

コマンド デフォルト

なし

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デバイスが 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、デバイス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、デバイス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。

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示します。つまり、同じドメイン内の 2 つのデバイスは、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。

```
Device# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf デバイス ID      Primary Server Revision   System Name
             lict
------------ ---- -------------- -------------- ---------- ----------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

次の例では、**show vtp counters** コマンドの出力を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
Device> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/0/47              0                0                0
Gi1/0/48              0                0                0
Gi2/0/1               0                0                0
Gi3/0/2               0                0                0
```

表 *59*：*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 ポート上でこのデバイスが受信するサマリー アドバタイズメントの数。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 ポート上でこのデバイスが受信するサブセット アドバタイズメントの数。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。

フィールド	説明
Request advertisements received	トランク ポート上でこのデバイスが受信するアドバタイズメント要求の数。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 ポート上でこのデバイスが送信するサマリー アドバタイズメントの数。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 ポート上でこのデバイスが送信するサブセット アドバタイズメントの数。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 transmitted	トランク ポート上でこのデバイスが送信するアドバタイズメント要求の数。アドバタイズ要求は、通常、すべてのVLAN上に関する情報を要求します。また、VLANのサブセットに関する情報も要求できます。
Number of configuration revision errors	リビジョン エラーの数。 新しいVLANの定義、既存VLANの削除、中断、または再開、あるいは既存VLANのパラメータ変更を行うと、デバイスのコンフィギュレーション リビジョン番号が増加します。 リビジョン番号がデバイス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メントをデバイスが受信すると、リビジョンエラーが増加します。このエラーは、2つのデバイスのVTPパスワードが異なるか、またはデバイスの設定が異なることを意味します。 これらのエラーは、デバイスが受信アドバタイズメントをフィルタしていて、これによりVTPデータベースがネットワーク全体で同期されていない状態になっていることを示しています。

フィールド	説明
Number of configuration digest errors	MD5 ダイジェスト エラーの数。 サマリー パケット内の MD5 ダイジェストと、デバイスによって計算された受信済みアドバタイズメントの 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 つのデバイスの 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、すべてのデバイスで VTP パスワードが同じになるようにします。 これらのエラーは、デバイスが受信アドバタイズメントをフィルタしていて、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。
Number of V1 summary errors	バージョン 1 エラーの数。 VTP V2 モードのデバイスが VTP バージョン 1 フレームを受信すると、バージョン 1 サマリー エラーが増加します。これらのエラーは、少なくとも 1 つの近接デバイスで、V2 モードがディセーブルにされた VTP バージョン 1、または VTP バージョン 2 が実行されていることを示しています。この問題を解決するには、VTP V2 モードのデバイス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、**show vtp status** コマンドの出力を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
Device> show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 2037.06ce.3580
```

```
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                                    0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

表 *60*：***show vtp status*** のフィールドの説明

フィールド	説明
VTP Version capable	デバイス上で動作できる VTP バージョンを表示します。
VTP Version running	デバイス上で動作中の VTP バージョンを表示します。デフォルトでは、デバイスはバージョン 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。
VTP Domain Name	デバイスの管理ドメインを特定する名前。
VTP Pruning Mode	プルーニングがイネーブルかまたはディセーブルかを表示します。VTP サーバでプルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。プルーニングを使用すると、トラフィックが適切なネットワークデバイスにアクセスするために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されます。
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。
Device ID	ローカル デバイスの MAC アドレスを表示します。
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デバイスの IP アドレスを表示します。

フィールド	説明
VTP Operating Mode	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。 **Server**：VTP サーバ モードのデバイスは VTP に対してイネーブルであり、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。このデバイスを使用すると、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、すべてのデバイスがVTPサーバです。 （注） デバイスが設定を NVRAM に書き込んでいる間に障害を検出し、NVRAM が機能するまでサーバ モードに戻ることができない場合、スイッチはVTP サーバ モードから VTP クライアント モードに自動的に変わります。 **Client**：VTP クライアント モードのデバイスは VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN設定を格納するために十分な不揮発性ストレージがありません。スイッチでは VLAN を設定できません。VTP クライアントが起動すると、VTP クライアントはそのVLANデータベースを初期化するアドバタイズを受信するまで、VTPアドバタイズを送信しません。 **Transparent**：VTP トランスペアレント モードのデバイスは、VTPに対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメントの学習を行いません。また、ネットワーク内の他のデバイスのVLAN設定にも影響しません。デバイスは VTP アドバタイズメントを受信し、アドバタイズメント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。
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。
Configuration Revision	このデバイスの現在のコンフィギュレーション リビジョン番号。

フィールド	説明
MD5 Digest	VTP 設定の 16 バイト チェックサム。

次の例では、VTP バージョン 3 を実行するデバイスに対する **show vtp status** コマンドの出力を示します。

```
Device> 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:
----------------
```

関連トピック

clear vtp counters, （1409 ページ）

show wireless vlan group

VLAN グループ内の VLAN の詳細リストと DHCP に失敗した VLAN のステータスを表示するには、特権 EXEC モードで **showwirelessvlangroup** コマンドを使用します。

show wireless vlan group *group-name*

構文の説明

group-name	ワイヤレス VLAN グループの名前。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、グローバル コンフィギュレーション モードでのみ使用してください。

次の例では、VLAN グループのサマリーを表示する方法を示します。

```
Device# show wireless vlan group grp1

Member Vlans Configured
------------------------------------------------------------
VLAN        VLAN Name                               DHCP Failed
100         VLAN0100                                No
101         VLAN0101                                Yes
102         VLAN0102                                No
103         VLAN0103                                No
104         VLAN0104                                Yes
105         VLAN0105                                No
```

switchport priority extend

着信したタグなしフレームのポート プライオリティ、または指定されたポートに接続された IP Phoneが受信するフレームのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **switchport priority extend** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport priority extend {**cos** *value*| **trust**}

no switchport priority extend

構文の説明

cos *value*	PC から受信したか、または指定した Class of Service（CoS）値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は0～7です。7が最も高いプライオリティです。デフォルトは 0 です。
trust	PC または接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。

コマンド 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

音声 VLAN をイネーブルにした場合、デバイスを設定して、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 に接続しているデバイスポートの 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 はすべてのデバイス インターフェイスでグローバルにイネーブルです）。

デバイス 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、**trust device cisco-phone** インターフェイス コンフィギュレーション コマンドを入力してインターフェイス上でサービス品質（QoS）をイネーブルに設定しておくことを推奨します。Auto QoS 機能を使用すると、これらは自動的に設定されます。

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。

```
Device(config)# interface gigabitethernet1/0/2
Device(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。

switchport trunk

インターフェイスがトランキング モードの場合、トランクの特性を設定するには、インターフェイス コンフィギュレーション モードで **switchport trunk** 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

allowed vlan *vlan-list*	トランキング モードの場合に、このインターフェイス上でタグ付き形式のトラフィックを送受信できる許可VLANのリストを設定します。*vlan-list* の選択については、「使用上のガイドライン」を参照してください。
native vlan *vlan-id*	インターフェイスが IEEE 802.1Q トランキング モードの場合に、タグなしトラフィックを送受信するようにネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です。
pruning vlan *vlan-list*	トランキング モードの場合に、VTP プルーニングに適格な VLAN のリストを設定します。*vlan-list* の選択については、「使用上のガイドライン」を参照してください。

コマンド 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
Cisco IOS XE 3.2SE	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** では、1 ～ 4094 のすべての VLAN を指定します。これはデフォルトです。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**：空のリストを指定します。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**：現在設定されている VLAN リストを置き換えるのではなく、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**：現在設定されている VLAN リストを置き換えずに、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。

- **except**：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（指定されている VLAN 以外の VLAN が追加されます）。有効な ID の範囲は 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：

- IEEE 802.1Q トランク ポートで受信されたすべてのタグなしトラフィックは、ポートに設定されたネイティブ VLAN によって転送されます。
- パケットの VLAN ID が送信側ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。
- **native vlan** コマンドの **no** 形式は、ネイティブ モード VLAN を、デバイスに適したデフォルト VLAN にリセットします。

許可 VLAN：

- スパニングツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol（CDP）、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、ダイナミック トランキング プロトコル（DTP）、および VLAN 1 の VLAN トランキング プロトコル（VTP））を送受信し続けます。
- リストをデフォルト リスト（すべての VLAN を許可）にリセットするには、**allowed vlan** コマンドの **no** 形式を使用します。

トランク プルーニング：

- プルーニング適格リストは、トランク ポートだけに適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLAN をプルーニングしない場合は、プルーニング適格リストから VLAN を削除します。プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。
- VLAN 1、VLAN 1002 ～ 1005、および拡張範囲 VLAN（VLAN 1006 ～ 4094）は、プルーニングできません。

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。

```
Device(config)# interface gigabitethernet1/0/2
Device(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。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーニング適格リストから VLAN 3 および 10 ～ 15 を削除する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(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。

関連トピック

show interfaces, （205 ページ）
switchport mode

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 を削除するには、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

vlan-id	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。
group **word vlan-list**	VLAN グループの作成をイネーブルにします。VLAN グループ名は最大 32 文字であり、文字で始める必要があります。

コマンド デフォルト

なし

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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。通常範囲の VLAN の設定情報は常に VLAN データベースに保存されます。この情報を表示するには、**show vlan** 特権 EXEC コマンドを入力します。VTP モードがトランスペアレントである場合、通常範囲の VLAN の VLAN 設定情報もデバイス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。拡張範囲の VLAN ID は VLAN データベースに保存されず、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。また、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、。VTP バージョン 1 および 2 で伝播する範囲は、VLAN 1 ～ 1005 だけです。

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デバイスをリブートすると、設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、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 コンフィギュレーション内の 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、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

無効な VLAN ID を入力すると、エラー メッセージが表示され、VLAN コンフィギュレーション モードを開始できません。

VLAN ID を指定して **vlan** コマンドを入力すると、VLAN コンフィギュレーション モードがイネーブルになります。既存の VLAN の VLAN ID を入力すると、新しい VLAN は作成されませんが、その VLAN の VLAN パラメータを変更できます。指定された VLAN は、VLAN コンフィギュレーション モードを終了したときに追加または変更されます。（VLAN 1 ～ 1005 の）**shutdown** コマンドだけがただちに有効になります。

（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 **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。

次のコンフィギュレーション コマンドをVLANコンフィギュレーション モードで利用できます。各コマンドの **no** 形式を使用すると、特性がそのデフォルト ステートに戻ります。

- **are** *are-number*：この VLAN の All-Route Explorer（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。デフォルト値は 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。
  - **enable**：この VLAN のバックアップ CRF モード。
  - **disable**：この VLAN のバックアップ CRF モード（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、すなわち 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 ブリッジング
  - **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 ）を増加させ、VLAN コンフィギュレーション モードを終了します。
- **media**：VLAN のメディア タイプを定義します。タイプは次のいずれかになります。

（注） デバイスは、イーサネット ポートだけをサポートします。FDDI およびトークン リング メディア固有の特性は、別のデバイスに対する VLAN Trunking Protocol（VTP）グローバル アドバタイズメントにかぎって設定します。これらの VLAN はローカルに停止されます。

  - **ethernet**：イーサネット メディア タイプ（デフォルト）。
  - **fd-net**：FDDI ネットワーク エンティティ タイトル（NET）メディア タイプ。
  - **fddi**：FDDI メディア タイプ。
  - **tokenring**：VTP v2 モードがディセーブルの場合は、トークン リング メディア タイプ。VTP バージョン 2（v）モードがイネーブルの場合は、TrCRF。
  - **tr-net**：VTP v2 モードがディセーブルの場合は、トークン リング ネットワーク エンティティ タイトル（NET）メディア タイプ。VTP v2 モードがイネーブルの場合は、TrBRF メディア タイプ。

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、下の表を参照してください。

- **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 を定義するときに必要です。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 スイッチド ポート アナライザ（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。

  （注） RSPAN 機能は、LAN Base イメージが稼働しているスイッチでだけサポートされます。

- **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 Security Association Identifier（SAID）を指定します。指定できる ID は、1 ～ 4294967294 です。この数字は、管理ドメイン内で一意である必要があります。デフォルト値は、100000 に VLAN ID 番号を加算した値です。
- **shutdown**：VLAN 上で VLAN スイッチングをシャットダウンします。このコマンドはただちに有効になります。他のコマンドは、VLAN コンフィギュレーション モードを終了したときに有効になります。
- **state**：VLAN ステートを指定します。
  - **active** は、VLAN が稼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）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。デフォルト値は 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。

- **ieee**：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。
- **ibm**：ソースルート ブリッジング（SRB）を実行している IBM STP。
- **auto**：ソースルート トランスペアレント ブリッジング（IEEE）およびソースルート ブリッジング（IBM）の組み合わせを実行している STP。

- **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 ***61***：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	**name***vlan-name*, **media ethernet**, **state** {**suspend** | **active**}, **said***said-value*, **remote-span**, **tb-vlan1***tb-vlan1-id*, **tb-vlan2***tb-vlan2-id*
FDDI	**name***vlan-name*, **media fddi**, **state** {**suspend** | **active**}, **said***said-value*, **ring***ring-number*, **parent***parent-vlan-id*, **tb-vlan1***tb-vlan1-id*, **tb-vlan2***tb-vlan2-id*
FDDI-NET	**name***vlan-name*, **media fd-net** , **state** {**suspend** | **active**}, **said***said-value*, **bridge***bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1***tb-vlan1-id*, **tb-vlan2***tb-vlan2-id* VTP v2 モードがディセーブルの場合、**stp type** を **auto** に設定しないでください。
Token Ring	VTP v1 モードはイネーブルです。 **name***vlan-name*, **media tokenring**, **state** {**suspend** | **active**}, **said***said-value*, **ring***ring-number*, **parent***parent-vlan-id*, **tb-vlan1***tb-vlan1-id*, **tb-vlan2***tb-vlan2-id*

メディア タイプ	指定できる構文
トークンリング コンセントレータ リレー機能（TrCRF）	VTP v2 モードはイネーブルです。 **name***vlan-name*, **media tokenring**, **state** {**suspend | active**}, **said***said-value*, **ring***ring-number*, **parent***parent-vlan-id*, **bridge type** {**srb | srt**}, **are***are-number*, **ste***ste-number*, **backupcrf** {**enable | disable**}, **tb-vlan1***tb-vlan1-id*, **tb-vlan2***tb-vlan2-id*
トークンリング NET	VTP v1 モードはイネーブルです。 **name***vlan-name*, **media tr-net**, **state** {**suspend | active**}, **said***said-value*, **bridge***bridge-number*, **stp type** {**ieee | ibm**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
トークンリングブリッジリレー機能（TrBRF）	VTP v2 モードはイネーブルです。 **name***vlan-name*, **media tr-net**, **state** {**suspend | active**}, **said***said-value*, **bridge***bridge-number*, **stp type** {**ieee | ibm | auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

次の表に、VLAN の設定ルールを示します。

表 *62*：*VLAN* 設定ルール

設定（**Configuration**）	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。 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。 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。

設定（Configuration）	ルール
VTP v1 モードはイネーブルです。	VLAN の STP タイプを auto に設定しないでください。 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。 （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 へのポインタが含まれている必要があります。 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。 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。

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 VLAN *xxxx* 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 は ethernet です。state は active です。デフォルトの said-value は、100000 に VLAN ID を加算した値です。mtu-size 変数は 1500、stp-type は ieee です。**exit** 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。

次に、新しい VLANをすべてデフォルトの特性で 作成し、VLAN コンフィギュレーション モードを開始する例を示します。

```
Device(config)# vlan 200
Device(config-vlan)# exit
Device(config)#
```

次に、新しい拡張範囲VLANをすべてデフォルトの特性で作成して、VLANコンフィギュレーション モードを開始し、新しい VLAN をデバイスのスタートアップ コンフィギュレーション ファイルに保存する例を示します。

```
Device(config)# vlan 2000
Device(config-vlan)# end
Device# copy running-config startup config
```

次に、VLAN グループを作成する例を示します。

```
Device(config)#  vlan group xyz vlan-list 50-60
```

次に、リモート VLAN グループを作成する例を示します。

```
Device(config)#  no vlan group xyz vlan-list 50-60
```

次に、1 つの VLAN を VLAN グループから削除する例を示します。

```
Device(config)#    no vlan group xyz vlan-list 51
```

次に、複数の VLAN を VLAN グループから削除する例を示します。

```
Device(config)#    no vlan group xyz vlan-list 52-55
```

次に、1 つの VLAN と複数の VLAN を VLAN グループから削除する例を示します。

```
Device(config)#    no vlan group xyz vlan-list 56, 58-60
```

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

関連トピック

show vlan, （1419 ページ）

vlan dot1q tag native

すべての IEEE 802.1Q トランク ポートでネイティブ VLAN フレームのタギングをイネーブルにするには、グローバル コンフィギュレーション モードで **vlan dot1q tag native** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vlan dot1q tag native

no vlan dot1q tag native

（注） このコマンドは、LAN Base イメージを実行しているデバイスではサポートされません。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IEEE 802.1Q ネイティブ VLAN タギングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

イネーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされます。

ディセーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされません。

IEEE 802.1Q トンネリングに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、ネイティブ VLAN フレームの IEEE 802.1Q タギングをイネーブルにする方法を示します。

```
Device# configure terminal
Device (config)# vlan dot1q tag native
Device (config)# end
```

設定を確認するには、**show vlan dot1q tag native** 特権 EXEC コマンドを入力します。

関連トピック

show vlan, （1419 ページ）

vtp（グローバル コンフィギュレーション）

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）設定の特性を設定するか、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 **vtp** コマンドを使用します。この設定を削除したりデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vtp {**domain** *domain-name*| **file** *filename*| **interface** *interface-name* [**only**]| **mode** {**client**| **off**| **server**| **transparent**} [**mst**| **unknown**| **vlan**]| **password** *password* [**hidden**| **secret**]| **pruning**| **version** *number*}

no vtp {**file**| **interface**| **mode** [**client**| **off**| **server**| **transparent**] [**mst**| **unknown**| **vlan**]| **password**| **pruning**| **version**}

構文の説明

domain *domain-name*	VTP ドメイン名をデバイスの VTP 管理ドメインを識別する 1 ～ 32 文字の ASCII 文字列で指定します。ドメイン名では大文字と小文字が区別されます。
file *filename*	VTP VLAN 設定が保存されている Cisco IOS ファイル システム ファイルを指定します。

interface *interface-name*	このデバイスで更新されたVTP IDを提供するインターフェイスの名前を指定します。
only	（任意）VTP IPアップデータとしてこのインターフェイスのIPアドレスだけを使用します。
mode	VTP デバイス 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。
client	デバイスを VTP クライアント モードにします。VTP クライアント モードのデバイスは VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN 設定を格納するための十分な不揮発性メモリがありません。VTP クライアントでは、VLAN を設定できません。VLAN は、ドメインに含まれる、他のサーバ モードのデバイスで設定します。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
off	デバイスを VTP オフ モードにします。VTP オフ モードのデバイスは、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。
server	デバイスを VTP サーバ モードにします。VTP サーバ モードのデバイスは 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。デバイスでは VLAN を設定できます。デバイスは、再起動後に、不揮発性メモリから現在の VTP データベース内のすべての VLAN 情報を回復できます。
transparent	デバイスを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デバイスは、VTP に対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメント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。デバイスは VTP アドバタイズメントを受信し、アドバタイズメントを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。 VTP モードが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デバイス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。この情報をデバイスのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup config** 特権 EXEC コマンドを入力します。
mst	（任意）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。
unknown	（任意）未知の VTP データベース（VTP バージョン 3 に限る）にモードを設定します。
vlan	（任意）VLAN VTP データベースにモードを設定します。これがデフォルトです（VTP バージョン 3 に限る）。

password *password*	VTP アドバタイズメントで送信され、受信 VTP アドバタイズメントを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ～ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。
hidden	（任意）パスワード文字列から生成されたキーが VLAN データベース ファイルに保存されることを指定します。**hidden** キーワードを指定しない場合、パスワード文字列はクリアテキストに保存されます。hidden パスワードを入力した場合、そのパスワードを再入力し、ドメイン内でコマンドを実行する必要があります。このキーワードは、VTP バージョン 3 だけでサポートされています。
secret	（任意）ユーザがパスワードの秘密キーを直接設定できるようにします（VTP バージョン 3 に限る）。
pruning	デバイス上で VTP プルーニングをイネーブルにします。
version *number*	VTP バージョンをバージョン 1、バージョン 2、またはバージョン 3 に設定します。

コマンド 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

VTPモード、ドメイン名、およびVLAN設定をデバイスのスタートアップ コンフィギュレーション ファイルに保存して、デバイスを再起動すると、VTPおよびVLAN設定は次の条件によって選択されます。

- スタートアップ コンフィギュレーションおよびVLANデータベース内のVTPモードがトランスペアレントであり、VLANデータベースとスタートアップ コンフィギュレーション ファイルのVTPドメイン名が一致する場合は、VLANデータベースが無視され（クリアされ）、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 コンフィギュレーション内の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、VLAN ID 1 ～ 1005 のドメイン名、VTPモード、およびVTP設定にはVLANデータベース情報が使用されます。

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、デバイスは非管理ドメイン ステートの状態です。非管理ドメイン ステートの間は、ローカルVLAN設定に変更が生じても、デバイスはVTPアドバタイズメントを送信しません。デバイスは、トランキングを行っているポートで最初のVTPサマリー パケットを受信した後、または **vtp domain** コマンドでドメイン名を設定した後で、非管理ドメイン ステートから抜け出します。デバイスは、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。デバイスが非管理ドメイン 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るしかありません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、デバイスを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、デバイスがクライアント 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。
- 受信デバイスがクライアント モードである場合、クライアント デバイスはその設定を変更して、サーバの設定をコピーします。クライアント モードのデバイスがある場合には、必ずサーバ モードのデバイスですべてのVTPまたはVLAN設定変更を行ってください。サーバ モードのスイッチの方が、保持しているVTPコンフィギュレーション リビジョン番号が大きいためです。受信デバイスがトランスペアレント モードの場合、そのデバイスの設定は変更されません。

- トランスペアレント モードのデバイスは、VTP に参加しません。トランスペアレント モードのデバイスで VTP または VLAN 設定の変更を行った場合、その変更はネットワーク内の他のデバイスには伝播されません。
- サーバ モードのデバイスで 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デバイスに伝播されます。
- **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、デバイス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、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 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ている場合には、VTP モードをクライアントまたはサーバに変更できません。VTP 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。
- 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。
- 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デバイスで一致している必要があります。
- デバイス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 デバイスは他のすべての 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 デバイスでバージョン 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設定する必要があります。
- ドメイン内のすべてのデバイスが VTP バージョン 2 対応である場合、1 つのデバイスでバージョン 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 対応デバイスに伝播されます。
- 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 情報がその VTP ドメイン全体に伝播します。
- VTP バージョン 3 の 2 つのリージョンが、VTP バージョン 1 または VTP バージョン 2 のリージョン経由で通信できるのは、トランスペアレントモードの場合に限られます。

デバイス 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。

次の例では、VTP コンフィギュレーション ストレージのファイル名を vtpfilename に変更する方法を示します。

```
Device(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。

```
Device(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。

```
Device(config)# vtp interface gigabitethernet
```

次の例では、デバイスの管理ドメインを設定する方法を示します。

```
Device(config)# vtp domain OurDomainName
```

次の例では、デバイスを VTP トランスペアレント モードにする方法を示します。

```
Device(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。

```
Device(config)# vtp password ThisIsOurDomainsPassword
```

次の例では、VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
Device(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。

```
Device(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。

関連トピック

show vtp, （1422 ページ）

vtp（インターフェイス コンフィギュレーション）, （1448 ページ）

vtp（インターフェイス コンフィギュレーション）

ポート単位で VLAN Trunking Protocol（VTP）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **vtp** 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には、このコマンドの **no** 形式を使用します。

vtp

no vtp

構文の説明

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
Cisco IOS XE 3.2SE	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、トランキング モードのインターフェイスでのみ入力してください。

このコマンドは、デバイス が VTP バージョン 3 を実行している場合にのみサポートされます。

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。

```
Device(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。

```
Device(config-if)# no vtp
```

関連トピック

switchport trunk, （1431 ページ）

vtp（グローバル コンフィギュレーション）, （1442 ページ）

vtp primary

デバイス を VLAN Trunking Protocol（VTP）プライマリ サーバとして設定するには、特権 EXEC モードで **vtp primary** コマンドを使用します。

vtp primary [**mst**| **vlan**][**force**]

構文の説明

mst	（任意）デバイス 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。
vlan	（任意）デバイス を VLAN のプライマリ VTP サーバとして設定します。
force	（任意）プライマリ サーバを設定するときにデバイス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。

コマンド デフォルト

デバイス 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

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。

（注） このコマンドは、デバイスが VTP バージョン 3 を実行している場合にのみサポートされます。

次の例では、デバイス 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。

```
Device# 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。

関連トピック

show vtp, （1422 ページ）

vtp（グローバル コンフィギュレーション）, （1442 ページ）

wireless broadcast vlan

VLAN 上でブロードキャストのサポー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 **wireless broadcast vlan** コマンドを使用します。イーサネット ブロードキャストのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

wireless broadcast vlan [*vlan-id*]

no wireless broadcast vlan [*vlan-id*]

構文の説明

vlan-id	（任意） VLAN ID を指定して、その VLAN に対するブロードキャスト サポートをイネーブルにします。値の範囲は 1 ～ 4095 です。

コマンド デフォルト

なし

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、グローバル コンフィギュレーション モードのみで使用してください。

次の例では、VLAN 20 でブロードキャスティングをイネーブルにする方法を示します。

```
Device(config)# wireless broadcast vlan 20
```

第 XXII 部

WLAN

- WLAN コマンド，1455 ページ

第 26 章

WLAN コマンド

- aaa-override, 1457 ページ
- accounting-list, 1458 ページ
- assisted-roaming, 1459 ページ
- ap name ap-name lan port-id port-id poe, 1460 ページ
- ap name ap-name lan override, 1461 ページ
- band-select, 1462 ページ
- broadcast-ssid, 1463 ページ
- call-snoop, 1464 ページ
- channel-scan defer-priority, 1465 ページ
- channel-scan defer-time, 1466 ページ
- chd, 1467 ページ
- client association limit, 1468 ページ
- client vlan, 1470 ページ
- ccx aironet-iesupport, 1471 ページ
- datalink flow monitor, 1472 ページ
- device-classification, 1473 ページ
- default, 1474 ページ
- dtim dot11, 1477 ページ
- exclusionlist, 1478 ページ
- exit, 1479 ページ
- exit（WLAN AP グループ）, 1479 ページ

- ip access-group, 1480 ページ
- ip flow monitor, 1481 ページ
- ip verify source mac-check, 1482 ページ
- load-balance, 1483 ページ
- mobility anchor, 1484 ページ
- nac, 1486 ページ
- passive-client, 1487 ページ
- peer-blocking, 1488 ページ
- port, 1489 ページ
- poe, 1490 ページ
- radio, 1490 ページ
- radio-policy, 1492 ページ
- remote-lan, 1493 ページ
- remote-lan, 1494 ページ
- roamed-voice-client re-anchor, 1494 ページ
- security ft, 1495 ページ
- security pmf, 1497 ページ
- security web-auth, 1498 ページ
- security wpa akm, 1499 ページ
- service-policy（WLAN）, 1501 ページ
- session-timeout, 1502 ページ
- show remote-lan all, 1503 ページ
- show remote-lan id, 1504 ページ
- show remote-lan name, 1505 ページ
- show remote-lan summary, 1506 ページ
- show running-config remote-lan, 1507 ページ
- show wlan, 1507 ページ
- show wireless wlan summary, 1510 ページ
- shutdown, 1511 ページ
- sip-cac, 1512 ページ
- static-ip tunneling, 1513 ページ

- vlan, 1514 ページ
- universal-admin, 1515 ページ
- wgb non-cisco, 1515 ページ
- wifidirect policy, 1516 ページ
- wlan（AP グループの設定）, 1517 ページ
- wlan, 1518 ページ
- wlan shutdown, 1519 ページ
- wmm, 1520 ページ

aaa-override

WLAN で AAA オーバーライドを有効にするには、**aaa-override** コマンドを使用します。AAA オーバーライドを無効にするには、このコマンドの **no** 形式を使用します。

aaa-override

no aaa-override

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。

コマンド デフォルト

デフォルトでは AAA が無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で AAA を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

次に、WLAN で AAA を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

accounting-list

WLAN で RADIUS アカウンティング サーバを設定するには、**accounting-list** コマンドを使用します。RADIUS サーバ アカウンティングを無効にするには、このコマンドの **no** 形式を使用します。

accounting-list *radius-server-acct*

no accounting-list

構文の説明

radius-server-acct	アカウンティング RADIUS サーバ名。

コマンド デフォルト

デフォルトでは RADIUS サーバ アカウンティングが無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で RADIUS サーバ アカウンティングを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# accounting-list test
Device(config-wlan)# end
```

次に、WLAN で RADIUS サーバ アカウンティングを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no accounting-list test
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

assisted-roaming

WLAN で 802.11k を使用して経由ローミングを設定するには、**assisted-roaming** コマンドを使用します。経由ローミングを無効にするには、このコマンドの **no** 形式を使用します。

assisted-roaming {**dual-list**| **neighbor-list**| **prediction**}

no assisted-roaming {**dual-list**| **neighbor-list**| **prediction**}

構文の説明

dual-list	WLANのデュアルバンド802.11kネイバーリストを設定します。デフォルトは、クライアントが現在関連付けられている帯域です。
neighbor-list	WLAN の 802.11k ネイバー リストを設定します。
prediction	WLAN の経由ローミング最適化の予測を設定します。

コマンド デフォルト

ネイバー リストとデュアル バンドのサポートはデフォルトで有効になっています。デフォルトは、クライアントが現在関連付けられている帯域です。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

経由ローミングの予測のリストを有効にすると、警告が表示されます。また、WLANでロードバランシングがすでに有効になっている場合、ロード バランシングはその WLAN で無効になります。WLAN に変更を加えるには、WLAN が無効状態になっている必要があります。

例

次に、WLAN で 802.11k ネイバー リストを設定する例を示します。

```
Device(config-wlan)#assisted-roaming neighbor-list
```

次に、WLANでロードバランシングが有効になっている場合の警告メッセージの例を示します。経由ローミングを設定するときにロード バランシングがすでに有効になっている場合は、ロードバランシングを無効にする必要があります。

```
Device(config)#wlan test-prediction 2 test-prediction
Device(config-wlan)#client vlan 43
Device(config-wlan)#no security wpa
Device(config-wlan)#load-balance
Device(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming
Prediction Optimization on this WLAN.
```

ap name ap-name lan port-id port-id poe

AP の LAN ポートで PoE を有効にするには、特権 EXEC モードで **ap name ap-name lan port-id port-id poe** コマンドを使用します。AP の LAN ポートで PoE を無効にするには、このコマンドの **no** 形式を使用します。

（注） PoE はポート 1 に対してのみ設定できます。

ap name *ap-name* **lan port-id** *port-id* **poe**

no ap name *ap-name* **lan port-id** *port-id* **poe**

構文の説明

ap-name	AP の名前。

port-id	ポートの ID。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、AP の LAN ポートで PoE を有効にする例を示します。

```
Switch # ap name AP00FE.C82D.DFB0 lan port-id 1 poe
```

ap name ap-name lan override

AP グループの LAN ポート設定でオーバーライドを有効にするには、特権 EXEC モードで **ap name ap-name lan override** コマンドを使用します。AP グループの LAN ポート設定でオーバーライドを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **lan override**

no ap name *ap-name* **lan override**

構文の説明

ap-name	AP の名前。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、AP グループの LAN ポート設定でオーバーライドを有効にする例を示します。

```
Switch # ap name AP00FE.C82D.DFB0 lan override
```

band-select

WLAN で帯域選択を設定するには、**band-select** コマンドを使用します。帯域選択を無効にするには、このコマンドの **no** 形式を使用します。

band-select

no band-select

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。

コマンド デフォルト

デフォルトでは、帯域選択は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

WLAN で帯域選択を有効にすると、アクセス ポイントによって 2.4 GHz でのクライアント プローブが抑制され、デュアル バンド クライアントが 5 GHz スペクトルに移動されます。帯域選択アルゴリズムによるデュアル バンド クライアントの誘導は、同じアクセス ポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で帯域選択を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# band-select
Device(config-wlan)# end
```

次に、WLAN で帯域選択を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no band-select
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

broadcast-ssid

WLAN でサービス セット識別子（SSID）を有効にするには、**broadcast-ssid** コマンドを使用します。SSID のブロードキャスティングを無効にするには、このコマンドの **no** 形式を使用します。

broadcast-ssid

no broadcast-ssid

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。

コマンド デフォルト

WLAN の SSID はデフォルトでブロードキャストされます。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN でブロードキャスト SSID を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# broadcast-ssid
Device(config-wlan)# end
```

次に、WLAN でブロードキャスト SSID を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no broadcast-ssid
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

call-snoop

WLAN で Voice over IP（VoIP）スヌーピングを有効にするには、**call-snoop** コマンドを使用します。Voice over IP（VoIP）を無効にするには、このコマンドの **no** 形式を使用します。

call-snoop

no call-snoop

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。

コマンド デフォルト

デフォルトでは VoIP スヌーピングは無効になっています。

コマンド モード

WLN 設定

使用上のガイドライン

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANを無効にする方法の詳細については、「関連コマンド」の項を参照してください。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

コール スヌーピングが設定される WLAN は、Platinum QoS で設定されている必要があります。このコマンドを使用する前に、QoS を無効にする必要があります。QoS サービス ポリシーの設定の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で VoIP を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# call-snoop
Device(config-wlan)# end
```

次に、WLAN で VoIP を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no call-snoop
Device(config-wlan)# end
```

関連トピック

service-policy（WLAN）, （893 ページ）

wlan, （1518 ページ）

channel-scan defer-priority

オフチャネル スキャンを延期できるパケットの優先順位マーキングに対して、延期するようにデバイスを設定するには、**channel-scandefer-priority** コマンドを使用します。オフチャネル スキャンを延期できるパケットの優先順位マーキングに対して、延期するデバイスを無効にするには、このコマンドの **no** 形式を使用します。

channel-scan defer-priority *priority*

no channel-scan defer-priority *priority*

構文の説明

priority	チャネル優先順位値。指定できる範囲は 0 ～ 7 です。デフォルトは 3 です。

コマンド デフォルト

WLAN の設定チャン延期が有効になっています。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、WLAN でチャネル スキャン延期優先順位を有効にして、それを優先順位値 4 に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# channel-scan defer-priority 4
Device(config-wlan)# end
```

次に、WLAN でチャネル スキャン延期優先順位を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no channel-scan defer-priority 4
Device(config-wlan)# end
```

channel-scan defer-time

チャネル スキャン延期時間を割り当てるには、**channel-scandefer-time** コマンドを使用します。チャネル スキャン延期時間を無効にするには、このコマンドの **no** 形式を使用します。

channel-scan defer-time *msecs*

no channel-scan defer-time

構文の説明

msecs	延期時間（ミリ秒単位）。値の範囲は 0 ～ 60000 です。デフォルトは 100 です。

コマンド デフォルト

チャネル スキャン延期時間が有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

ミリ秒単位の時間値は、WLAN 機器の要件を満たす必要があります。

次に、WLAN でチャネル スキャンを有効にして、スキャン延期時間を 300 ミリ秒に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# channel-scan defer-time 300
Device(config-wlan)# end
```

次に、WLAN でチャネル スキャン延期時間を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no channel-scan defer-time
Device(config-wlan)# end
```

chd

WLAN でカバレッジ ホール検出を有効にするには、**chd** コマンドを使用します。カバレッジ ホール検出を無効にするには、このコマンドの **no** 形式を使用します。

chd

no chd

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。

コマンド デフォルト

カバレッジ ホール検出が有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、WLAN でカバレッジ ホール検出を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# chd
Device(config-wlan)# end
```

次に、WLAN でカバレッジ ホール検出を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no chd
Device(config-wlan)# end
```

client association limit

WLAN のクライアント接続、アクセス ポイントあたりのクライアント、または無線アクセス ポイントあたりのクライアントの最大数を設定するには、**clientassociationlimit** コマンドを使用します。WLAN のクライアント アソシエーションの上限を無効にするには、このコマンドの **no** 形式を使用します。

client association limit {*association-limit*| **ap** *ap-limit*| **radio** *max-ap-radio-limit*}

no client association limit {*association-limit*| **ap** *ap-limit*| **radio** *max-ap-radio-limit*}

構文の説明

association-limit	許可されるクライアント接続の数。有効な範囲は 0 ～ 2000 です。値がゼロ（0）の場合、上限が設定されていないことを示します。
ap	アクセスポイントあたりのクライアントの最大数。
ap-limit	無線アクセスポイントあたりに許可されるクライアント接続の最大数を設定します。有効な範囲は 0 ～ 400 です。

radio	無線 AP あたりのクライアントの最大数を設定します。
max-ap-radio-limit	無線アクセスポイントあたりに許可されるクライアント接続の最大数。有効な範囲は 0 ～ 200 です。

コマンド デフォルト

クライアント接続の最大数は 0 （上限なし）に設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	コマンドが変更されました。**ap** キーワードと **radio** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント アソシエーションの制限を設定し、クライアントの上限を 200 に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# client association limit 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

次に、WLAN のクライアント アソシエーションの制限をディセーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no client association limit
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

次に、WLANの無線あたりのクライアントアソシエーションの制限を設定し、クライアントの上限を 200 に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit radio 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

次に、WLAN の AP あたりのクライアント アソシエーションの制限を設定し、クライアントの上限を 300 に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit ap 300
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

client vlan

WLAN インターフェイスまたはインターフェイス グループを設定するには、**clientvlan** コマンドを使用します。WLAN インターフェイ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。

client vlan *interface-id-name-or-group-name*

no client vlan

構文の説明

interface-id-name-or-group-name	インターフェイス ID、名前、または VLAN グループ名。インターフェイス ID は、複数桁で指定することもできます。

コマンド デフォルト

デフォルト インターフェイスが設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント VLAN をイネーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client vlan client-vlan1
Device(config-wlan)# end
```

次に、WLAN 上のクライアント VLAN をディセーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no client vlan
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

ccx aironet-iesupport

WLAN で Aironet 情報要素（IE）を有効にするには、**ccxaironet-iesupport** コマンドを使用します。Aironet 情報要素（IE）を無効にするには、このコマンドの **no** 形式を使用します。

ccx aironet-iesupport

no ccx aironet-iesupport

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。

コマンド デフォルト

Aironet IE サポートは有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で Aironet IE を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ccx aironet-iesupport
Device(config-wlan)# end
```

次に、WLAN で Aironet IE を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ccx aironet-iesupport
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

datalink flow monitor

WLAN での NetFlow モニタリングを有効にするには、**datalinkflowmonitor** コマンドを使用します。NetFlow モニタリングを無効にするには、このコマンドの **no** 形式を使用します。

datalink flow monitor *datalink-monitor-name* {**input**| **output**}

no datalink flow monitor *datalink-monitor-name* {**input**| **output**}

構文の説明

datalink-monitor-name	フロー モニタ名。データリンク モニタ名には最大 31 文字を含めることができます。
input	入力トラフィックの NetFlow モニタを指定します。
output	出力トラフィックの NetFlow モニタを指定します。

コマンド デフォルト

なし。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN での NetFlow モニタリングを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# datalink flow monitor test output
Device(config-wlan)# end
```

次に、WLAN での NetFlow モニタリングを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no datalink flow monitor test output
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

device-classification

WLAN でクライアント デバイスの分類を有効にするには、**device-classification** コマンドを使用します。デバイスの分類を無効にするには、このコマンドの **no** 形式を使用します。

device-classification

no device-classification

構文の説明

device-classification	クライアント デバイスの分類を有効または無効にします。

コマンド デフォルト

なし。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# device-classification
Device(config-wlan)# end
```

default

パラメータをデフォルト値に設定するには、**default** コマンドを使用します。

default {**aaa-override**| **accounting-list**| **band-select**| **broadcast-ssid**| **call-snoop**| **ccx**| **channel-scan**| **parameters**| **chd**| **client**| **datalink**| **diag-channel**| **dtim**| **exclusionlist**| **ip**| **ipv6**| **load-balance**| **local-auth**| **mac-filtering**| **media-stream**| **mfp**| **mobility**| **nac**| **passive-client**| **peer-blocking**| **radio**| **roamed-voice-client**| **security**| **service-policy**| **session-timeout**| **shutdown**| **sip-cac**| **static-ip**| **uapsd**| **wgb**| **wmm**}

構文の説明

aaa-override	AAAオーバーライドパラメータをデフォルト値に設定します。
accounting-list	アカウンティングパラメータとその属性をデフォルト値に設定します。
band-select	帯域選択パラメータをデフォルト値に設定します。
broadcast-ssid	ブロードキャストのサービスセット識別子（SSID）パラメータをデフォルト値に設定します。
call-snoop	コール スヌープ パラメータをデフォルト値に設定します。
ccx	Cisco Client Extension（Cisco Aironet IE）のパラメータと属性をデフォルト値に設定します。
channel-scan	チャネルスキャンのパラメータと属性をデフォルト値に設定します。
chd	カバレッジ ホール検出パラメータをデフォルト値に設定します。
client	クライアントのパラメータと属性をデフォルト値に設定します。
datalink	データリンクのパラメータと属性をデフォルト値に設定します。

diag-channel	診断チャネルのパラメータと属性をデフォルト値に設定します。
dtim	Delivery Traffic Indicator Message（DTIM）パラメータをデフォルト値に設定します。
exclusionlist	クライアント除外タイムアウトパラメータをデフォルト値に設定します。
ip	IP パラメータをデフォルト値に設定します。
ipv6	IPv6 のパラメータと属性をデフォルト値に設定します。
load-balance	ロードバランシング パラメータをデフォルト値に設定します。
local-auth	Extensible Authentication Protocol（EAP）プロファイルのパラメータと属性をデフォルト値に設定します。
mac-filtering	MAC フィルタリングのパラメータと属性をデフォルト値に設定します。
media-stream	メディア ストリームのパラメータと属性をデフォルト値に設定します。
mfp	管理フレーム保護（MPF）のパラメータと属性をデフォルト値に設定します。
mobility	モビリティのパラメータと属性をデフォルト値に設定します。
nac	RADIUS ネットワーク アドミッション コントロール（NAC）パラメータをデフォルト値に設定します。
passive-client	パッシブ クライアント パラメータをデフォルト値に設定します。
peer-blocking	ピアツーピア ブロッキングのパラメータと属性をデフォルト値に設定します。
radio	ワイヤレス ポリシーのパラメータと属性をデフォルト値に設定します。
roamed-voice-client	ローミングされた音声クライアントのパラメータと属性をデフォルト値に設定します。
security	セキュリティ ポリシーのパラメータと属性をデフォルト値に設定します。

service-policy	WLAN サービス品質（QoS）ポリシーのパラメータと属性をデフォルト値に設定します。
session-timeout	クライアント セッション タイムアウト パラメータをデフォルト値に設定します。
shutdown	シャットダウン パラメータをデフォルト値に設定します。
sip-cac	Session Initiation Protocol（SIP）のコール アドミッション制御（CAC）のパラメータと属性をデフォルト値に設定します。
static-ip	スタティック IP クライアント トンネリングのパラメータと属性をデフォルト値に設定します。
uapsd	Wi-Fi マルチメディア（WMM）不定期自動省電力配信（UAPSD）のパラメータと属性をデフォルト値に設定します。
wgb	ワークグループブリッジ（WGB）パラメータをデフォルト値に設定します。
wmm	WMM のパラメータと属性をデフォルト値に設定します。

コマンド デフォルト

なし。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、Cisco Client Extensio パラメータをデフォルト値に設定する例を示します。

```
Device(config-wlan)# default ccx aironet-iesupport
```

関連トピック

wlan, （1518 ページ）

dtim dot11

WLAN の Delivery Traffic Indicator Message（DTIM）期間を設定するには、**dtimdot11** コマンドを使用します。DTIM を無効にするには、このコマンドの **no** 形式を使用します。

dtim dot11 {**5ghz**| **24ghz**}*dtim-period*

no dtim dot11 {**5ghz**| **24ghz**}*dtim-period*

構文の説明

5ghz	5 GHz 帯域の DTIM 期間を設定します。
24ghz	2.4 GHz 帯域の DTIM 期間を設定します。
dtim-period	DTIM 期間の値。範囲は 1 ～ 255 です。

コマンド デフォルト

DTIM 期間は 1 に設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で DTIM 期間を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# dtim dot11 24ghz 3
```

次に、2.4 GHz 帯域の WLAN で DTIM 期間を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no dtim dot11 24ghz 3
```

関連トピック

wlan, （1518 ページ）

exclusionlist

無線 LAN で除外リストを設定するには、**exclusionlist** コマンドを使用します。除外リストを無効にするには、このコマンドの **no** 形式を使用します。

exclusionlist [**timeout** *seconds*]

no exclusionlist [timeout]

構文の説明

timeout*seconds*	（任意）除外リスト タイムアウトを秒単位で指定します。指定できる範囲は 0 ～ 2147483647 です。値ゼロ（0）はタイムアウトなしを示します。

コマンド デフォルト

除外リストは 60 秒に設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント除外リストを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
```

```
Device(config-wlan)# exclusionlist timeout 345
```

次に、WLAN のクライアント除外リストを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no exclusionlist timeout 345
```

exit

WLAN コンフィギュレーション サブモードを終了するには、**exit** コマンドを使用します。

exit

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。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、WLAN コンフィギュレーション サブモードを終了する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# exit
Device(config)#
```

exit（WLAN AP グループ）

WLAN アクセスポイント グループ サブモードを終了するには、**exit** コマンドを使用します。

exit

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。

コマンド デフォルト

WLAN AP グループ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、WLAN AP グループ サブモードを終了する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap group test
Device(config-apgroup)# exit
```

ip access-group

WLAN アクセス コントロール グループ（ACL）を設定するには、**ipaccess-group** コマンドを使用します。WLAN ACL 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 [web] *acl-name*

no ip access-group [web]

構文の説明

web	（任意）IPv4 Web ACL を設定します。
acl-name	セキュリティ タイプ値を webauth として、WLAN に使用する preauth ACL を指定します。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

使用上のガイドライン

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、WLAN ACL を設定する例を示します。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wlan wlan1
Device(config-wlan)#ip access-group test-acl
```

次に、IPv4 WLAN Web ACL を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip access-group web test
Device(config-wlan)#
```

関連トピック

wlan, （1518 ページ）

ip flow monitor

IP NetFlow モニタリングを設定するには、**ipflowmonitor** コマンドを使用します。IP NetFlow モニタリ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 flow monitor *ip-monitor-name* {**input**| **output**}

no ip flow monitor *ip-monitor-name* {**input**| **output**}

構文の説明

ip-monitor-name	フロー モニタ名。
input	入力トラフィックのフロー モニタを有効にします。
output	出力トラフィックのフロー モニタを有効にします。

コマンド デフォルト

なし

コマンド モード

使用上のガイドライン

WLAN の設定
このコマンドを使用する前に、WLAN をディセーブルにする必要があります。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、入力トラフィックに IP フロー モニタを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip flow monitor test input
```

次に、IP フロー モニタを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ip flow monitor test input
```

ip verify source mac-check

WLAN の IPv4 ソース ガード（IPSG）を有効にするには、**ipverifysourcemac-check** コマンドを使用します。IPSG を無効にするには、このコマンドの **no** 形式を使用します。

ip verify source mac-check

no ip verify source mac-check

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。

コマンド デフォルト

IPSG は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

ホストのIPアドレスに基づいて、ホストから特定のインターフェイスへのトラフィックを制限するには、この機能を使用します。機能は、IPスプーフィングを防ぐために、ホストの送信元MACとIPをバインドするように設定することもできます。

DHCPスヌーピング、ARPおよびDataglean から受信した情報に基づいて、ワイヤレス ホストのIPアドレスとMACアドレスをバインドするには、この機能を使用します。Datagleanは、DHCPリレーエージェントによってDHCPメッセージが転送された場合に、それらのメッセージからホストハードウェアアドレス、ホストに接続されているポートなどのロケーション情報を抽出するプロセスです。 ワイヤレス ホストが、デバイスによって学習されていないIPアドレスとMACアドレスの組み合わせを持つトラフィックの送信を試みた場合、このトラフィックはハードウェアでドロップされます。IPSGは、DHCPパケットではサポートされていません。IPSGは、外部デバイスの外部クライアントではサポートされていません。

このコマンドを使用する前に、WLANをディセーブルにする必要があります。

次に、IPSG を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip verify source mac-check
```

次に、IPSG を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ip verify source mac-check
```

load-balance

WLANのロードバランシングを有効にするには、**load-balance**コマンドを使用します。ロードバランシングを無効にするには、このコマンドの **no** 形式を使用します。

load-balance

no load-balance

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。

コマンド デフォルト

ロード バランシングはデフォルトではディセーブルになっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN でロード バランシングを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# shutdown
Device(config)# wlan wlan1
Device(config-wlan)# load-balance
Device(config)# no shutdown
Device(config-wlan)# end
```

次に、WLAN でロード バランシングを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# shutdown
Device(config)# wlan wlan1
Device(config-wlan)# no load-balance
Device(config)# no shutdown
Device(config-wlan)# end
```

関連トピック

wlan, （1518 ページ）

mobility anchor

モビリティ スティッキ アンカリングを設定するには、**mobility anchor sticky** コマンドを使用します。スティッキ アンカリングを無効にするには、このコマンドの **no** 形式を使用します。

ゲスト アンカリングを設定するには、**mobility anchor***ip-address* コマンドを使用します。

ゲスト アンカーを削除するには、このコマンドの **no** 形式を使用します。

デバイスを自動アンカーとして設定するには、**mobility anchor** コマンドを使用します。

mobility anchor {*ip-address*| **sticky**}

no mobility anchor {*ip-address*| **sticky**}

構文の説明

sticky	クライアントは、関連付けられている最初のスイッチにアンカーされます。 （注） このコマンドはデフォルトで有効になっており、低ローミング遅延を保証します。これは、クライアントがモビリティ ドメインに参加し、ドメイン内をローミングする場合でも、クライアントの Point of Presence のが変更されないように確保します。
ip-address	ゲスト アンカー デバイスの IP アドレスをこの WLAN に設定します。

コマンド デフォルト

スティッキ設定は、デフォルトでは有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE リリースより前の自動アンカー設定ではデバイス IP アドレスを入力する必要がありました。このリリースでは、IP アドレスが指定されていない場合、デバイス自身がアンカーになります。明示的に IP アドレスを指定する必要はありません。

使用上のガイドライン

- wlan_id または guest_lan_id は必ず指定し、無効にする必要があります。
- 1 つ目のモビリティ アンカーを設定するときに、WLAN または有線ゲスト LAN で自動アンカー モビリティを有効にします。
- 最後のアンカーを削除すると、自動アンカー モビリティ機能は無効になり、新しいアソシエーションに対しては標準のモビリティが再度使用されるようになります。
- モビリティは、ファイアウォールの通過が許可されている次のポートを使用します。
  - 16666
  - 16667
  - 16668

次に、スティッキ モビリティ アンカーを有効にする例を示します。
```
Device(config-wlan)# mobility anchor sticky
```

次に、ゲスト アンカリングを設定する例を示します。
```
Device(config-wlan)# mobility anchor 209.165.200.224
```

次に、デバイスを自動アンカーとして設定する例を示します。
```
Device(config-wlan)# mobility anchor
```

nac

WLAN 対応の RADIUS ネットワーク アドミッション コントロール（NAC）サポートを有効にするには、**nac** コマンドを使用します。NAC アウトオブバンド サポートを無効にするには、このコマンドの **no** 形式を使用します。

nac

no nac

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。

コマンド デフォルト

NAC は無効です。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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 NAC 状態を有効にする前に、AAA オーバーライドを有効にする必要があります。

次に、WLAN に RADIUS NAC を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# aaa-override
Device(config-wlan)# nac
```

次に、WLAN で RADIUS NAC を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no nac
Device(config-wlan)# no aaa-override
```

関連トピック

aaa-override, （1457 ページ）

passive-client

WLAN のパッシブ クライアント機能を有効にするには、**passive-client** コマンドを使用します。パッシブ クライアント機能を無効にするには、このコマンドの **no** 形式を使用します。

passive-client

no passive-client

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。

コマンド デフォルト

パッシブ クライアント機能は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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、グローバル マルチキャスト モードとマルチキャスト-マルチキャスト モードを有効にする必要があります。マルチキャスト-マルチキャスト モードとマルチキャスト-ユニキャスト モードの両方がサポートされています。マルチキャスト-マルチキャスト モードが推奨されます。

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN でパッシブ クライアント機能を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast
Device(config)# wlan test-wlan
Device(config-wlan)# passive-client
```

次に、WLAN でパッシブ クライアント機能を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast
Device(config)# wlan test-wlan
Device(config-wlan)# no passive-client
```

関連トピック

wlan, （1518 ページ）

peer-blocking

WLANにピアツーピア ブロッキング機能を設定するには、**peer-blocking**コマンドを使用します。ピアツーピア ブロッキング機能を無効にするには、このコマンドの **no** 形式を使用します。

peer-blocking {**drop**| **forward-upstream**}

no peer-blocking

構文の説明

drop	デバイスでパケットを破棄するように指定します。
forward-upstream	パケットがアップストリーム VLAN に転送されるように指定します。デバイスの次に上の階層のデバイスが、パケットに関して実行するアクションを決定します。

コマンド デフォルト

ピア ブロッキングは無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、ピアツーピア ブロッキングの drop オプションと forward-upstream オプションを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# peer-blocking  drop
Device(config-wlan)# peer-blocking forward-upstream
```

次に、ピアツーピア ブロッキングの drop オプションと forward-upstream オプションを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no peer-blocking  drop
Device(config-wlan)# no peer-blocking forward-upstream
```

関連トピック

wlan, （1518 ページ）

port

AP グループのポート ID 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 **port** コマンドを使用します。AP グループのポート ID を無効にするには、このコマンドの **no** 形式を使用します。

port *port-id*

no port *port-id*

構文の説明

port-id	ポートの ID。

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（config-apgroup）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、AP グループのポート ID を設定する例を示します。

```
Switch(config-apgroup)# port-1
```

poe

ポートで PoE を有効にするには、インターフェイス コンフィギュレーション モードで **poe** コマンドを使用します。ポートで PoE を無効にするには、このコマンドの **no** 形式を使用します。

（注） PoE はポート 1 に対してのみ設定できます。

poe

no poe

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（config-apgroup）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、ポートで PoE を有効にする方法を示します。

```
Switch(config-apgroup)# poe
```

radio

WLAN のシスコ無線ポリシーを有効にするには、**radio** コマンドを使用します。WLAN のシスコ無線ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

radio {**all**| **dot11a**| **dot11ag**| **dot11bg**| **dot11g**}

no radio

構文の説明

all	すべての無線帯域で WLAN を設定します。
dot11a	802.11a の無線帯域だけに WLAN を設定します。
dot11ag	802.11a/g の無線帯域に WLAN を設定します。
dot11bg	802.11b/g 無線帯域だけに無線 LAN を設定します（802.11g が無効な場合は 802.11b だけに設定）。
dot11g	802.11g の無線帯域だけに無線 LAN を設定します。

コマンド デフォルト

無線ポリシーは、すべての帯域で有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、すべての無線帯域に無線 LAN を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# radio all
```

次に、WLAN 上のすべての無線帯域を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no radio all
```

関連トピック

wlan, （1518 ページ）

radio-policy

WLAN アクセス ポイント グループに無線ポリシーを設定するには、**radio-policy** コマンドを使用します。WLAN の無線ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

radio-policy {**all**| **dot11a**| **dot11bg**| **dot11g**}

no radio{**all**| **dot11a**| **dot11bg**| **dot11g**}

構文の説明

all	すべての無線帯域で無線 LAN を設定します。
dot11a	802.11a 無線帯域だけに無線 LAN を設定します。
dot11bg	802.11b/g だけに無線 LAN を設定します（802.11g が無効な場合は 802.11b だけに設定）。
dot11g	802.11g 無線帯域だけに無線 LAN を設定します。

コマンド デフォルト

無線ポリシーは、すべての帯域で有効になっています。

コマンド モード

WLAN AP グループ 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

変更を有効にするには、NTP サービスを再起動する必要があります。WLAN をシャットダウンする方法の詳細については、「関連コマンド」の項を参照してください。

次に、AP グループの 802.11b 帯域で無線ポリシーを有効にする例を示します。

```
Device(config)# ap group test
Device(config-apgroup)# wlan test-wlan
```

```
Device(config-wlan-apgroup)# radio-policy dot11b
```

次に、AP グループの 802.11b 帯域で無線ポリシーを無効にする例を示します。

```
Device(config)# ap group test
Device(config-apgroup)# wlan test-wlan
Device(config-wlan-apgroup)# no radio-policy dot11bg
```

関連トピック

wlan, （1518 ページ）

wlan shutdown, （1519 ページ）

remote-lan

リモート LAN プロ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 **remote-lan** コマンドを使用します。設定したプロファイル名を無効にするには、このコマンドの **no** 形式を使用します。

remote-lan *profile-name id*

no remote-lan *profile-name id*

構文の説明

profile-name	リモート LAN プロファイル名。
id	リモート LAN の識別子。範囲は 1 ～ 64 です。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、リモート LAN プロファイル名を指定する例を示します。

```
Switch(config)# remote-lan test-lan 3
```

remote-lan

リモート LAN を AP グループに追加するには、インターフェイス コンフィギュレーション モードで **remote-lan** コマンドを使用します。AP グループ内のリモート LAN を無効にするには、このコマンドの **no** 形式を使用します。

remote-lan *remote-lan-name*

no remote-lan *remote-lan-name*

（注） **remote-lan remote-lan-name** コマンドは、リモート LAN をポートにマッピングする際にも必要です。

構文の説明

remote-lan-name	リモート LAN の名前。

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（config-apgroup）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、リモート LAN を AP グループに追加する例を示します。

```
Switch(config-apgroup)# remote-lan test-lan
```

roamed-voice-client re-anchor

ローミングしている音声クライアントのリアンカー機能を有効にするには、**roamed-voice-clientre-anchor** コマンドを使用します。ローミングしている音声クライアントのリアンカー機能を向こうにするには、このコマンドの **no** 形式を使用します。

roamed-voice-client re-anchor

no roamed-voice-client re-anchor

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。

コマンド デフォルト

ローミングしている音声クライアントのリアンカー機能は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次にローミングしている音声クライアントのリアンカー機能を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# roamed-voice-client re-anchor
```

次にローミングしている音声クライアントのリアンカー機能を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no roamed-voice-client re-anchor
```

関連トピック

wlan, （1518 ページ）

security ft

802.11r Fast Transition パラメータを設定するには、**security ft** コマンドを使用します。**over the air**（無線）の Fast Transition を設定するには、**no security ft over-the-ds** コマンドを使用します。

security ft [**over-the-ds**| **reassociation-timeout** *timeout-jn-seconds*]

no security ft [**over-the-ds**| **reassociation-timeout**]

構文の説明

over-the-ds	（任意）802.11r Fast Transition が分散システムを介して発生するように指定します。このパラメータを指定したコマンドの no 形式は、無線を介したセキュリティ Fast Transition を設定します。
reassociation-timeout	（任意）再アソシエーションのタイムアウト間隔を設定します。
timeout-in-seconds	（任意）再アソシエーションのタイムアウト間隔を秒単位で指定します。有効な範囲は 1 ～ 100 です。デフォルト値は 20 です。

コマンド デフォルト

機能はディセーブルです。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし

WLAN セキュリティを有効にする必要があります。

例

次に、オープンな WLAN のセキュリティ FT を設定する例を示します:

```
Device#wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no mobility anchor sticky
Device(config-wlan)# no security wpa
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# no security wpa wpa2 ciphers aes
Device(config-wlan)# security ft
Device(config-wlan)# shutdown
```

次に、WPA 対応の WLAN のセキュリティ FT を表示する例を示します。

```
Device# wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no security wpa akm dot1x
```

```
Device(config-wlan)# security wpa akm ft psk
Device(config-wlan)# security wpa akm psk set-key ascii 0 test-test
Device(config-wlan)# security ft
Device(config-wlan)# no shutdown
```

security pmf

WLAN に 802.11w 管理フレーム保護（PMF）を設定するには、**security pmf** コマンドを使用します。管理フレーム保護を無効にするには、このコマンドの **no** 形式を使用します。

security pmf {**association-comeback** *association-comeback-time-seconds*| **mandatory**| **optional**| **saquery-retry-time** *saquery-retry-time-milliseconds*}

no security pmf [**association-comeback** *association-comeback-time-seconds*| **mandatory**| **optional**| **saquery-retry-time** *saquery-retry-time-milliseconds*]

構文の説明

association-comeback	802.11w アソシエーション復帰時間を設定します。
association-comeback-time-seconds	アソシエーション復帰間隔（秒単位）。アソシエーションがステータス コード 30 によって拒否された後に、アソシエートされているクライアントがアソシエーションを再試行するまでに待機する必要がある時間間隔。ステータス コード 30 のメッセージは、「Association request rejected temporarily; Try again later」です。 有効範囲は 1 ～ 20 秒です。
mandatory	クライアントが WLAN の 802.1w PMF 保護をネゴシエートする必要があることを指定します。
optional	WLAN がクライアントでの 802.11w サポートを必要としていないことを指定します。802.11w機能のないクライアントも、参加可能です。
saquery-retry-time	SA クエリの応答を受け取るまでの時間。デバイスが応答を受け取らなかった場合、別の SA クエリーが試行されます。
saquery-retry-time-milliseconds	SA クエリの再試行時間は、ミリ秒単位で指定します。指定できる範囲は 100 ～ 500 ミリ秒です。値には 100 ミリ秒の倍数を指定する必要があります。

コマンド デフォルト

PMF は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

この機能を使用するには、WPA（Wi-Fi Protected Access）と AKM（認証キー管理）が設定されている必要があります。セキュリティ パラメータの設定の詳細については、「関連コマンド」の項を参照してください。

802.11w では、ブロードキャストまたはマルチキャストの堅牢な管理フレームを保護するために使用される Integrity Group Temporal Key（IGTK）が導入されています。IGTK は、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用するオーセンティケータ ステーション（デバイス）によって割り当てられる、ランダムな値です。802.11w IGTK キーは、4 ウェイ ハンドシェイクを使用して取得され、レイヤ 2 で WPA2 セキュリティが設定されている WLAN でのみ使用されます。

次に、アソシエーション復帰時間値を 15 秒で有効にする例を示します。

```
Device(config-wlan)# security pmf association-comeback 15
```

次に、WLAN のクライアントに必須の 802.11w MPF 保護を設定する例を示します。

```
Device(config-wlan)# security pmf mandatory
```

次に、WLAN のクライアントにオプションの 802.11w MPF 保護を設定する例を示します。

```
Device(config-wlan)# security pmf optional
```

次に、saquery パラメータを設定する例を示します。

```
Device(config-wlan)# security pmf saquery-retry-time 100
```

次に、PMF 機能を無効にする例を示します。

```
Device(config-wlan)# no security pmf
```

関連トピック

security wpa akm, （1499 ページ）

security web-auth

WLAN で使用する Web 認証のステータスを変更するには、**securityweb-auth** コマンドを使用します。WLAN で Web 認証を無効にするには、このコマンドの **no** 形式を使用します。

security web-auth [**authentication-list** *authentication-list-name*| **on-macfilter-failure**| **parameter-map** *parameter-map-name*]

no security web-auth [**authentication-list [authentication-list-name]| on-macfilter-failure**| **parameter-map [parameter-name]**]

構文の説明

authentication-list*authentication-list-name*	IEEE 802.1x の認証リストを設定します。

on-macfilter-failure	MAC の失敗時の Web 認証を有効にします。
parameter-map*parameter-map-name*	パラメータ マップを設定します。

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

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

例

次に、WLAN に認証リストによる Web 認証を設定する例を示します。

```
Device(config-wlan)# security web-auth authentication-list test
```

security wpa akm

Cisco Centralized Key Management（CCKM）を使用して認証キー管理を設定するには、**security wpa akm** コマンドを使用します。Cisco Centralized Key Management の認証キー管理を無効にするには、このコマンドの **no** 形式を使用します。

security wpa [**akm** {**cckm**| **dot1x**| **ft**| **pmf**| **psk**}| **wpa1** [**ciphers** {**aes**| **tkip**}]| **wpa2** [**ciphers** {**aes**| **tikp**}]]

no security wpa [**akm** {**cckm**| **dot1x**| **ft**| **pmf**| **psk**}| **wpa1** [**ciphers** {**aes**| **tkip**}]| **wpa2** [**ciphers** {**aes**| **tikp**}]]

構文の説明

akm	認証キー管理（AKM）パラメータを設定します。
aes	AES（Advanced Encryption Standard）暗号化サポートを設定します。

cckm	Cisco Centralized Key Management のサポートを設定します。
ciphers	WPA 暗号方式を設定します。
dot1x	802.1x のサポートを設定します。
ft	802.11r を使用して Fast Transition を設定します。
pmf	802.11w 管理フレーム保護を設定します。
psk	802.11r Fast Transition の事前共有キー（PSK）のサポートを設定します。
tkip	Temporal Key Integrity Protocol（TKIP）暗号化のサポートを設定します。
wpa2	Wi-Fi Protected Access 2（WPA2）のサポートを設定します。

コマンド デフォルト

デフォルトでは Wi-Fi Protected Access2、802.1x は有効になっています。WPA2、PSK、CCKM、FT dot1x、FT PSK、PMF dot1x、PMF PSK、FT のサポートは無効になっています。FT の再アソシエーションのタイムアウトは 20 秒、PMF SA クエリ時間は 200 に設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、WLAN に CCKM を設定する例を示します。

```
Device(config-wlan)#security wpa akm cckm
```

service-policy（WLAN）

WLAN サービス品質（QoS）サービス ポリシーを設定するには、**service-policy** コマンドを使用します。WLAN の QoS ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

service-policy [client] {**input| output**}*policy-name*

no service-policy [client] {**input| output**}*policy-name*

構文の説明

client	（任意）WLAN 上のすべてのクライアントにポリシー マップを割り当てます。
input	入力ポリシー マップを割り当てます。
output	出力ポリシー マップを割り当てます。
policy-name	ポリシー名。

コマンド デフォルト

ポリシーが割り当てられない場合、ポリシーに割り当てられる状態は [None] になります。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次の例では、WLAN の入力 QoS サービス ポリシーを設定する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy input policy-test
```

次の例では、WLAN の入力 QoS サービス ポリシーをディセーブルにする方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no service-policy input policy-test
```

次に、WLAN の出力 QoS サービス ポリシーを platinum（貴金属ポリシー）に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy output platinum
```

関連トピック

wlan, （1518 ページ）

wlan, （1518 ページ）

session-timeout

WLANに関連付けられたクライアントのセッションタイムアウトを設定するには、**session-timeout** コマンドを使用します。WLANに関連付けられたクライアントのセッションタイムアウトを無効にするには、このコマンドの **no** 形式を使用します。

session-timeout seconds

no session-timeout

構文の説明

seconds	タイムアウトまたはセッション時間（秒）。値 0 は、タイムアウトなしに相当します。範囲は 300 ～ 86400 です。

コマンド デフォルト

dot1x セキュリティが設定された WLAN の場合、クライアントのタイムアウトは 1800 秒に設定されます。オープンな WLAN の場合、クライアントのタイムアウトは 0 に設定されます。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、セッション タイムアウトを 300 秒に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# session-timeout 300
```

次に、セッション タイムアウトを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no session-timeout
```

show remote-lan all

設定済みのすべてのリモート LAN のリモート LAN プロパティを表示するには、**show remote-lan all** コマンドを使用します。

show remote-lan all

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。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、設定済みのすべてのリモート LAN のリモート LAN プロパティを表示する例を示します。

```
Switch#show remote-lan all
Remote-LAN Profile Name : test
```

```
================================================
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
802.11 Authentication : Open System
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

show remote-lan id

ID 別にリモート LAN 設定を表示するには、**show remote-lan id** コマンドを使用します。

show remote-lan id *id*

構文の説明

id	リモート LAN の識別子。範囲は 1 ～ 64 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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、ID 別にリモート LAN 設定を表示する例を示します。

```
Switch #show remote-lan id 2
Remote-LAN Profile Name     : test
================================================
Identifier                                    : 2
Status                                        : Disabled
Universal AP Admin                            : Disabled
Max Associated Clients per Remote-LAN         : 0
AAA Policy Override                           : Enabled
Number of Active Clients                      : 0
Exclusionlist Timeout                         : 21474
Session Timeout                               : 864 seconds
Interface                                     : default
Interface Status                              : Up
Remote-LAN ACL                                 : testacl
DHCP Server                                   : 10.5.7.9
DHCP Address Assignment Required              : Disabled
Local EAP Authentication                      : testeapprofile
Mac Filter Authorization list name            : testmaclist
Accounting list name                          : testlist
802.1x authentication list name               : dotxauth
Security
    802.11 Authentication                     : Open System
    802.1X                                    : Enabled
        Encryption                            : 104-bit WEP
```

show remote-lan name

プロファイル名別にリモート LAN 設定を表示するには、**show remote-lan name** コマンドを使用します。

show remote-lan name *name*

構文の説明

name	リモート LAN プロファイル名。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、プロファイル名別にリモート LAN 設定を表示する例を示します。

```
Switch# show remote-lan name test
Remote-LAN Profile Name : test
================================================
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
802.11 Authentication : Open System
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

show remote-lan summary

すべてのリモート LAN のサマリーを表示するには、**show remote-lan summary** コマンドを使用します。

show remote-lan summary

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。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、すべてのリモート LAN のサマリーを表示する例を示します。

```
Switch # show remote-lan summary
Number of Remote-LANs: 1

Remote-LAN Profile Name                      VLAN Status
-----------------------------------------------------
2          test                              1    DOWN
```

show running-config remote-lan

リモート LAN 設定を表示するには、**show running-config remote-lan** コマンドを使用します。

show running-config remote-lan *name*

構文の説明

name	リモート LAN プロファイル名。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、リモート LAN 設定を表示する例を示します。

```
Switch# show running-config remote-lan test
remote-lan test 1
aaa-override
accounting-list test-all-list
exclusionlist timeout 100
ip access-group test-acl
ip dhcp server 10.100.12.5
mac-filtering test-mac-list
security dot1x authentication-list test-dot1x-list
session-timeout 100
shutdown
```

show wlan

WLAN パラメータを表示するには、**show wlan** コマンドを使用します。

show wlan {**all** | **id** *wlan-id*| **name** *wlan-name* | **summary**}

構文の説明

all	すべての設定済みWLANのパラメータのサマリーを表示します。リストはWLAN IDの昇順に表示されます。
id *wlan-id*	無線LANの識別子を指定します。範囲は1～512です。
name *wlan-name*	WLANプロファイル名を指定します。名前は1～32文字です。
summary	WLANに設定されているパラメータのサマリーを表示します。

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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、デバイスに設定されている WLAN のサマリーを表示する例を示します。

```
Device# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                              VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                        test-wlan-ssid                     1    UP
```

次に、特定の WLAN に設定されているパラメータのサマリーを表示する例を示します。

```
Device# show wlan name test-wlan
WLAN Identifier                               : 45
Profile Name                                  : test-wlan
Network Name (SSID)                           : test-wlan-ssid
Status                                        : Enabled
Broadcast SSID                                : Enabled
Maximum number of Associated Clients          : 0
AAA Policy Override                           : Disabled
Network Admission Control
  NAC-State                                   : Disabled
Number of Active Clients                      : 0
Exclusionlist Timeout                         : 60
Session Timeout                               : 1800 seconds
CHD per WLAN                                  : Enabled
```

```
Webauth DHCP exclusion                           : Disabled
Interface                                        : default
Interface Status                                 : Up
Multicast Interface                              : test
WLAN IPv4 ACL                                    : test
WLAN IPv6 ACL                                    : unconfigured
DHCP Server                                      : Default
DHCP Address Assignment Required                 : Disabled
DHCP Option 82                                   : Disabled
DHCP Option 82 Format                            : ap-mac
DHCP Option 82 Ascii Mode                        : Disabled
DHCP Option 82 Rid Mode                          : Disabled
QoS Service Policy - Input
  Policy Name                                    : unknown
  Policy State                                   : None
QoS Service Policy - Output
  Policy Name                                    : unknown
  Policy State                                   : None
QoS Client Service Policy
  Input  Policy Name                             : unknown
  Output Policy Name                             : unknown
WifiDirect                                       : Disabled
WMM                                              : Disabled
Channel Scan Defer Priority:
  Priority (default)                             : 4
  Priority (default)                             : 5
  Priority (default)                             : 6
Scan Defer Time (msecs)                          : 100
Media Stream Multicast-direct                    : Disabled
CCX - AironetIe Support                          : Enabled
CCX - Gratuitous ProbeResponse (GPR)             : Disabled
CCX - Diagnostics Channel Capability             : Disabled
Dot11-Phone Mode (7920)                          : Invalid
Wired Protocol                                   : None
Peer-to-Peer Blocking Action                     : Disabled
Radio Policy                                     : All
DTIM period for 802.11a radio                    : 1
DTIM period for 802.11b radio                    : 1
Local EAP Authentication                         : Disabled
Mac Filter Authorization list name               : Disabled
Accounting list name                             : Disabled
802.1x authentication list name                  : Disabled
Security
    802.11 Authentication                        : Open System
    Static WEP Keys                              : Disabled
    802.1X                                       : Disabled
    Wi-Fi Protected Access (WPA/WPA2)            : Enabled
        WPA (SSN IE)                             : Disabled
        WPA2 (RSN IE)                            : Enabled
            TKIP Cipher                          : Disabled
            AES Cipher                           : Enabled
        Auth Key Management
            802.1x                               : Enabled
            PSK                                  : Disabled
            CCKM                                 : Disabled
    IP Security                                  : Disabled
    IP Security Passthru                         : Disabled
    L2TP                                         : Disabled
    Web Based Authentication                     : Disabled
    Conditional Web Redirect                     : Disabled
    Splash-Page Web Redirect                     : Disabled
    Auto Anchor                                  : Disabled
    Sticky Anchoring                             : Enabled
    Cranite Passthru                             : Disabled
    Fortress Passthru                            : Disabled
    PPTP                                         : Disabled
    Infrastructure MFP protection                : Enabled
    Client MFP                                   : Optional
    Webauth On-mac-filter Failure                : Disabled
    Webauth Authentication List Name             : Disabled
    Webauth Parameter Map                        : Disabled
    Tkip MIC Countermeasure Hold-down Timer      : 60
Call Snooping                                    : Disabled
```

```
Passive Client                                  : Disabled
Non Cisco WGB                                   : Disabled
Band Select                                     : Disabled
Load Balancing                                  : Disabled
IP Source Guard                                 : Disabled
Netflow Monitor                                 : test
        Direction                               : Input
        Traffic                                 : Datalink

Mobility Anchor List
IP Address
-----------
```

show wireless wlan summary

ワイヤレス WLAN のサマリーを表示するには、**show wireless wlan summary** コマンドを使用します。

show wireless wlan summary

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。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
15.2(3)E	このコマンドが導入されました。

次に、**show wireless wlan summary** コマンドの出力例を示します。

```
Cisco-Controller# show wireless wlan summary

Total WLAN Configured: 3

Total Client Count: 0


ID    Profile Name          SSID                 Security    Radio       VLAN        Client
   Status
-------------------------------------------------------------------------------------------------
1     Test1                 xxx                   WPA1/WPA2   All         1           0
     DOWN
2     wlan1                 wlan2-ssid            WPA1/WPA2   All         1           0
     DOWN
3     wlan3                 mywlan3               WPA1/WPA2   All         1           0
     DOWN
```

shutdown

WLAN を無効にするには、**shutdown** コマンドを使用します。WLAN を有効にするには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

（注） AP グループ設定とリモート LAN プロファイルの LAN ポートを有効にするには、このコマンドの **no** 形式を使用します。

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。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、WLAN を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan test-wlan
Device(config-wlan)# shutdown
Device(config-wlan)# end
Device# show wlan summary
Number of WLANs: 1

WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                        test-wlan-ssid                   1    DOWN
```

次に、WLAN を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan test-wlan
Device(config-wlan)# no shutdown
```

```
Device(config-wlan)# end
Device# show wlan summary
Number of WLANs: 1

WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                        test-wlan-ssid                  1    UP
```

sip-cac

WLAN の Session Initiation Protocol（SIP）コール アドミッション制御（CAC）機能を設定するには、**sip-cac** コマンドを使用します。SIP CAC 機能を無効にするには、このコマンドの **no** 形式を使用します。

sip-cac {**disassoc-client**| **send-486busy**}

no sip-cac {**disassoc-client**| **send-486busy**}

構文の説明

disassoc-client	CAC に障害が発生した場合に、クライアント関連付けの解除を有効にします。
send-486busy	CAC に障害が発生した場合に、SIP 486 ビジー メッセージを送信します。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN 上でクライアント関連付けの解除および 486 ビジー メッセージを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# sip-cac disassoc-client
Device(config-wlan)# sip-cac send-486busy
```

次に、WLAN 上でクライアント関連付けおよび 486 ビジー メッセージを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no sip-cac disassoc-client
Device(config-wlan)# no sip-cac send-486busy
```

関連トピック

wlan, （1518 ページ）

static-ip tunneling

WLAN のスタティック IP トンネリング機能を有効にするには、**static-ip tunneling** コマンドを使用します。スタティック IP トンネリング機能を無効にするには、このコマンドの **no** 形式を使用します。

static-ip tunneling

no static-ip tunneling

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。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

次に、スタティック IP トンネリングを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# static-ip tunneling
```

次に、スタティック IP トンネリングを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no static-ip tunneling
```

vlan

AP グループに VLAN を割り当てるには、**vlan** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。

vlan *interface-name*

no vlan

構文の説明

interface-name	VLAN インターフェイス名。

コマンド デフォルト

VLAN が AP グループに割り当てられていません。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

コマンド モード

WLAN AP グループの設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLAN をディセーブルにする必要があります。

次の例では、AP グループで VLAN を設定する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap group ap-group-1
```

```
Device(config-apgroup)# wlan test-wlan
Device(config-wlan-apgroup)# vlan 3
```

関連トピック

wlan, （1518 ページ）

universal-admin

WLAN をユニバーサル管理として設定するには、**universal-admin** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

universal-admin

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

```
Deviceenable
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wlan wlan1
Device(config-wlan)#universal-admin
```

wgb non-cisco

WLAN でシスコ以外のワークグループ ブリッジ（WGB）クライアントを有効にするには、**wgbnon-cisco** コマンドを使用します。シスコ以外の WGB クライアントのサポートを無効にするには、このコマンドの **no** 形式を使用します。

wgb non-cisco

構文の説明

no wgb non-cisco

WLAN の設定 WGB クライアントは無効にあります。

コマンド デフォルト

WLAN の設定 WGB クライアントは無効にあります。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN でシスコ以外の WGB を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# wgb non-cisco
Device(config-wlan)# no shutdown
```

次に、WLAN でシスコ以外の WGB クライアントのサポートを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no wgb non-cisco
Device(config-wlan)# no shutdown
```

wifidirect policy

WLAN で Wi-Fi Direct クライアント ポリシーを設定するには、**wifidirect policy** コマンドを使用します。Wi-Fi Direct クライアント ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

wifidirect policy {**permit**| **deny**}

構文の説明

permit	Wi-Fi Direct クライアントを有効にして WLAN と関連付けます。

deny	Wi-Fi Direct ポリシーが「拒否」に設定されている場合は、デバイス機能に基づいてデバイスが Wi-Fi Direct デバイスを許可または拒否します。Wi-Fi Direct デバイスは、関連付け要求でこれらの機能をデバイスにレポートします。これは、このデバイスの Wi-Fi 機能に基づいて行われます。次の作業を行います。 • 同時操作 • 相互接続 Wi-Fiデバイスが同時操作または相互接続、あるいはその両方をサポートする場合は、クライアントの関連付けは拒否されます。クライアントは、デバイスが同時操作と相互接続をサポートしない場合に関連付けることができます。

コマンド デフォルト

Wi-Fi Direct を無効にします。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、Wi-Fi Direct を有効にし、Wi-Fi Direct クライアントを設定して WLAN に関連付ける例を示します。

```
Device(config-wlan)# wifidirect policy permit
```

wlan（AP グループの設定）

アクセスポイント（AP）グループの WLAN の WLAN パラメータを設定するには、**wlan** コマンドを使用します。AP グループから WLAN を削除するには、このコマンドの **no** 形式を使用します。

wlan *wlan-name*

no wlan *wlan-name*

構文の説明

wlan-name	WLAN プロファイル名入力できる範囲は英数字で 1 ～ 32 文字です。

コマンド デフォルト

WLAN パラメータは、APグループに対して設定されていません。

コマンド モード

AP グループの設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、AP グループ コンフィギュレーション モードで WLAN 関連パラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap group test
Device(config-apgroup)# wlan qos-wlan
```

関連トピック

wlan, （1518 ページ）

wlan

無線 LAN を作成するには、**wlan** コマンドを使用します。無線 LAN 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。

wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

no wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

構文の説明

wlan-name	WLAN プロファイル名名前には、1 ～ 32 文字の英数字を使用できます。
wlan-id	無線 LAN の ID。範囲は 1 ～ 512 です。

wlan-ssid	SSID。入力できる範囲は英数字で 1 ～ 32 文字です。

コマンド デフォルト

WLAN 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
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

SSID を指定しない場合は、プロファイル名パラメータがプロファイル名と SSID の両方に使用されます。管理インターフェイスおよび AP マネージャ インターフェイスが同じポートにマップされており、いずれも同じ VLAN のメンバである場合は、WLAN を無効にしてから、ポートマッピングをいずれかのインターフェイスに変更する必要があります。管理インターフェイスと AP マネージャ（アクセス ポイント マネージャ）インターフェイスが別々の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。

アクセス ポイント グループに割り当てられている WLAN を削除しようとすると、エラー メッセージが表示されます。そのまま続行すると、アクセス ポイント グループとアクセス ポイントの無線から WLAN が削除されます。

次の例では、WLAN を作成する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config)# wlan test-wlan-cr 67 test-wlan-cr-ssid
```

次の例では、WLAN を削除する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config)# no wlan test-wlan-cr 67 test-wlan-cr-ssid
```

wlan shutdown

WLAN を無効にするには、**wlanshutdown** コマンドを使用します。WLAN フェイスを有効にするには、このコマンドの **no** 形式を使用します。

wlan shutdown

no wlan shutdown

コマンド デフォルト

WLAN は無効になっています。

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
Cisco IOS XE 3.2SE	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前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN をシャット ダウンする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
```

関連トピック

wlan, （1518 ページ）

wmm

WLANでWi-Fiマルチメディア（WMM）を有効にするには、**wmm**コマンドを使用します。WLANで WMM を無効にするには、このコマンドの **no** 形式を使用します。

wmm {**allowed**| **require**}

no wmm

構文の説明

allowed	WLAN での WMM の使用を許可します。
require	クライアントが WLAN で WMM を使用することを要求します。

コマンド デフォルト

WMMは無効になっています。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デバイスがレイヤ 2 モードで、WMM が有効化されている場合にアクセス ポイントをデバイスに結合できるようにするには、これらのアクセスポイントをトランク ポート上に配置する必要があります。

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で WMM を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# wmm allowed
```

次に、WLAN で WMM を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no wmm
```

関連トピック

wlan, （1518 ページ）

索 引

A

aaa-override コマンド 1457
access-session mac-move deny コマンド 1026
accounting-list コマンド 1458
action コマンド 1027
airtime-fairness 953
ap airtime-fairness policy 977
ap auth-list ap-policy 499
ap bridging 500
ap capwap multicast 501
ap capwap retransmit 502
ap capwap timers 503
ap cdp 505
ap core-dump 506
ap country 507
ap crash-file 508
ap dot11 2.4 GHz CleanAir アラーム デバイス 51
ap dot11 24ghz 509
ap dot11 24ghz cleanair 41
ap dot11 24ghz cleanair コマンド 39, 40, 42, 52
ap dot11 24ghz dot11g 510
ap dot11 24ghz rrm coverage コマンド 942
ap dot11 24ghz または 5ghz rrm channel dca add コマンド 939
ap dot11 24ghz または 5ghz rrm channel dca remove number 940
ap dot11 5ghz channelswitch mode 511
ap dot11 5ghz cleanair 32, 33
ap dot11 5ghz cleanair コマンド 34, 35, 48
ap dot11 5ghz power-constraint 512
ap dot11 5ghz rrm channel dca chan-width-11n 941
ap dot11 5ghz rrm channel device コマンド 38
ap dot11 5ghz rrm group-member コマンド 943
ap dot11 5ghz rrm profile コマンド 945
ap dot11 5ghz rrm tpc-threshold コマンド 946
ap dot11 5ghz rrm txpower コマンド 947
ap dot11 5ghz rrm コマンド 934
ap dot11 airtime-fairness 24ghz 5ghz device type コマンド 952
ap dot11 airtime-fairness policy device type コマンド 973, 978
ap dot11 beaconperiod 513
ap dot11 beamforming 514
ap dot11 cac media-stream 515
ap dot11 cac video 519
ap dot11 cac voice 520
ap dot11 cleanair 524
ap dot11 cleanair alarm air-quality 525
ap dot11 cleanair alarm device 525
ap dot11 cleanair device 527
ap dot11 dot11n 528
ap dot11 dtpc 531
ap dot11 dual-band cleanair 575
ap dot11 edcs-parameters 532
ap dot11 l2roam rf-params 535
ap dot11 media-stream 537
ap dot11 multimedia 517
ap dot11 rrm ccx location-measurement 538
ap dot11 rrm ccx コマンド 936
ap dot11 rrm channel cleanair-event 534
ap dot11 rrm channel dca 539
ap dot11 rrm channel コマンド 36, 45, 46, 937
ap dot11 rrm group-member 541
ap dot11 rrm group-mode 533
ap dot11 rrm logging 542
ap dot11 rrm monitor 543
ap dot11 rrm monitor mode コマンド 944
ap dot11 rrm ndp-type 544
ap dot11 コマンド 1397
ap dot1x max-sessions 546
ap dot1x username 547
ap ethernet duplex 548
ap group 549
ap image 550
ap led 552
ap link-encryption 553
ap link-latency 553
ap mgmtuser username 554
ap name 49ghz rrm profile 568
ap name ap-groupname 556
ap name bhrate 558
ap name bridgegroupname 558
ap name bridging 559
ap name capwap retransmit 562

ap name command 563
ap name console-redirect 561
ap name core-dump 564
ap name country 565
ap name crash-file 566
ap name dot11 24ghz rrm coverage 567
ap name dot11 5ghz rrm channel 570
ap name dot11 airtime-fairness wlan コマンド 954
ap name dot11 antenna 571
ap name dot11 antenna extantgain 572
ap name dot11 cleanair 573
ap name dot11 dot11n antenna 574
ap name dot11 rrm ccx 576
ap name dot11 rrm profile 577
ap name dot11 txpower 579
ap name dot1xuser 580
ap name ethernet 581
ap name ethernet duplex 582
ap name image 584
ap name led 588
ap name link-encryption 588
ap name link-latency 589
ap name location 590
ap name mgmtuser 591
ap name mode 592
ap name monitor-mode 594
ap name monitor-mode dot11b 595
ap name name 596
ap name no cdp interface 560
ap name no dot11 shutdown 596
ap name no telnet 602
ap name power injector 603
ap name power pre-standard 604
ap name power コマンド 597
ap name reset 605
ap name reset-button 604
ap name shutdown 598
ap name slot 606
ap name slot shutdown 599
ap name sniff 600
ap name ssh 601
ap name static-ip 607
ap name stats-timer 609
ap name syslog host 609
ap name syslog level 610
ap name tcp-adjust-mss 611
ap name tftp-downgrade 612
ap power injector 613
ap power pre-standard 614
ap reporting-period 615
ap reset-button 615
ap static-ip 617
ap syslog 618
ap tcp-adjust-mss size 620
ap tftp-downgrade 621
arp コマンド 1239
assisted-roaming コマンド 1459
authentication mac-move permit コマンド 1030
authentication priority コマンド 1032
auto qos classify コマンド 836
auto qos trust コマンド 842
auto qos video コマンド 849
auto qos voip コマンド 859

B

band-select コマンド 1462
boot コマンド 1240
broadcast-ssid コマンド 1463

C

cache コマンド 69
cache-memory-max コマンド 340
call-snoop コマンド 1464
cat コマンド 1241
ccx aironet-iesupport コマンド 1471
channel-group コマンド 412
channel-protocol コマンド 416
channel-scan defer-priority コマンド 1465
channel-scan defer-time コマンド 1466
chd コマンド 1467
Cisco Discovery Protocol（CDP） 1431
Cisco Mobility Services Engine（MSE） 169
cisp enable 1036
class コマンド 874
class-map コマンド 877
clear ap config 624
clear ap eventlog-all 625
clear ap join statistics 625
clear ap mac-address 626
clear ap name tsm dot11 all 623
clear ap name wlan statistics 627
clear errdisable interface vlan 1038
clear ip mfib コマンド 341
clear ip mroute コマンド 343
clear lacp コマンド 418
clear location statistics コマンド 1243
clear location コマンド 1242
clear mac address-table コマンド 1039

clear nmsp statistics コマンド 1244
clear pagp コマンド 419
clear spanning-tree counters コマンド 420
clear spanning-tree detected-protocols コマンド 421
clear vtp counters コマンド 1409
clear wireless ccx statistics コマンド 1244
clear wireless client tsm dot11 コマンド 1245
clear wireless location s69 statistics コマンド 1246
clear wireless mobility statistics 710
client association limit コマンド 1468
client vlan コマンド 141, 1408, 1470
collect counter コマンド 75
collect interface コマンド 76
collect timestamp absolute コマンド 77
collect transport tcp flags コマンド 79
collect コマンド 74
copy コマンド 1247

D

datalink flow monitor コマンド 80, 1472
debug ap mac-address 628
debug auto qos コマンド 872
debug etherchannel コマンド 422
debug flow exporter コマンド 81
debug flow monitor コマンド 82
debug ilpower コマンド 142
debug interface コマンド 144
debug lacp コマンド 424
debug lldp packets コマンド 145
debug nmsp コマンド 146
debug pagp コマンド 425
debug platform pm コマンド 426
debug platform poe コマンド 147
debug platform stack-manager コマンド 1170
debug platform udld コマンド 428
debug platform vlan コマンド 1409
debug spanning-tree コマンド 429
debug sw-vlan ifs コマンド 1412
debug sw-vlan notification コマンド 1413
debug sw-vlan vtp コマンド 1415
debug sw-vlan コマンド 1410
default ap dot11 rrm channel 50
default ap dot11 rrm channel cleanair-event 49
default ap dot11 rrm channel コマンド 55
default コマンド 1474
delete コマンド 1254
deny コマンド 1049
description コマンド 85
destination コマンド 86
device-classification コマンド 1473
dir コマンド 1255
dot1x supplicant force-multicast コマンド 1060
dot1x test timeout 1063
dscp コマンド 87
dtim dot11 コマンド 1477
duplex コマンド 148

E

emergency-install コマンド 1257
epm access-control open コマンド 1066
errdisable detect cause コマンド 150
errdisable recovery cause コマンド 152
errdisable recovery interval コマンド 155
exclusionlist コマンド 1478
exit コマンド 1259, 1479
export-protocol netflow-v9 コマンド 88

F

flash_init コマンド 1260
full-ring 状態 1215

H

help コマンド 1260

I

interface port-channel コマンド 431
interface range コマンド 157
interface vlan コマンド 1416
interface コマンド 156
ip access-group コマンド 1480
ip admission name コマンド 1070
ip device tracking maximum コマンド 1072
ip device tracking probe コマンド 1074
ip dhcp snooping verify no-relay-agent-address 1078
ip flow monitor コマンド 93, 1481
ip igmp snooping last-member-query-count コマンド 349
ip mtu コマンド 159

ip multicast auto-enable コマンド 357
ip multicast vlan コマンド 358
ip verify source mac-check コマンド 1482
ip verify source コマンド 1082
ipv6 flow monitor コマンド 95, 405
ipv6 mtu コマンド 160
ipv6 traffic-filter コマンド 406

L

lacp max-bundle コマンド 432
lacp port-priority コマンド 434
lacp system-priority コマンド 436
license right-to-use 1261
lldp（インターフェイス コンフィギュレーション）コマンド 161
load-balance コマンド 1483
location algorithm コマンド 1267
location expiry コマンド 1268
location notify-threshold コマンド 1269
location plm calibrating コマンド 1270
location rfid コマンド 1271
location rssi-half-life コマンド 1272
logging event power-inline-status コマンド 163

M

mab request format attribute 32 コマンド 1090
mac address-table move update コマンド 1273
main-cpu コマンド 1171
match datalink ethertype コマンド 96
match datalink mac コマンド 98
match datalink vlan コマンド 99
match flow direction コマンド 101
match interface コマンド 102
match ipv4 destination address コマンド 104
match ipv4 source address コマンド 105
match ipv4 ttl コマンド 106
match ipv4 コマンド 103
match ipv6 destination address コマンド 108
match ipv6 hop-limit コマンド 109
match ipv6 source コマンド 110
match ipv6 コマンド 107
match non-client-nrt コマンド 882
match transport icmp ipv4 コマンド 112
match transport icmp ipv6 コマンド 113
match transport コマンド 111
match wlan user-priority コマンド 883
match（アクセス マップ コンフィギュレーション）コマンド 1092
match（クラスマップ コンフィギュレーション）コマンド 879
mdix auto コマンド 164
media-stream multicast-direct コマンド 1400
mgmt_init コマンド 1274
mkdir コマンド 1275
mobility anchor 699, 1484
mode（電源スタックの設定）コマンド 165
monitor session filter コマンド 775
monitor session source コマンド 777
monitor session コマンド 769, 770
more コマンド 1276

N

nac コマンド 1486
network-policy profile（グローバル コンフィギュレーション）コマンド 168
network-policy profiles 223
network-policy コマンド 167
network-policy コンフィギュレーション モード 168
nmsp attachment suppress コマンド 169
nmsp notification interval コマンド 1277
no authentication logging verbose 1095
no dot1x logging verbose 1096
no mab logging verbose 1097

O

option コマンド 116

P

pagp learn-method コマンド 437
pagp port-priority コマンド 439
partial-ring 状態 1215
passive-client コマンド 1487
peer-blocking コマンド 1488
permit コマンド 1098
policy config-sync prc reload command 1173
policy weight airtime-fairness 949
policy-map コマンド 883

port-channel auto コマンド 441
port-channel load-balance extended コマンド 444
port-channel load-balance コマンド 442
port-channel min-links コマンド 445
power efficient-ethernet auto コマンド 170
power inline police コマンド 177
power inline コマンド 173
power supply コマンド 179
power-priority コマンド 171

Q

queue-limit コマンド 890

R

radio コマンド 1490
radio-policy コマンド 1492
redistribute mdns-sd コマンド 370
redundancy config-sync mismatched-commands command 1175
redundancy force-switchover コマンド 1177
redundancy reload コマンド 1178
redundancy コマンド 1174
reload コマンド 1179
rename コマンド 1279
request platform software trace archive 1390, 1391
request platform software trace filter binary 1392
reset コマンド 1280
rmdir コマンド 1281
roamed-voice-client re-anchor コマンド 1494
RSPAN 769, 770, 775, 777
  sessions 769, 770, 777
    インターフェイス追加 769, 770, 777
    新規開始 769, 770, 777

S

sdm prefer コマンド 1282
security passthru コマンド 1108
security web-auth コマンド 1498
service-list mdns-sd service-list-name コマンド 371
service-policy コマンド 374, 891, 893, 1501
service-policy-query コマンド 373
service-routing mdns-sd コマンド 373
session コマンド 1180
session-timeout コマンド 1502
set platform software trace 1378, 1382
set trace capwap ap ha コマンド 1181
set trace mobility ha コマンド 1183
set trace qos ap ha コマンド 1185
set コマンド 894, 1283
show airtime-fairness wlan type device コマンド 979
show ap airtime-fairness ap-group device type コマンド 976
show ap cac voice 628
show ap capwap 630
show ap cdp 631
show ap config dot11 632
show ap config fnf 633
show ap config global 634
show ap crash-file 635
show ap data-plane 635
show ap dot11 637, 638
show ap dot11 24ghz cleanair summary コマンド 63
show ap dot11 24ghz cleanair デバイス タイプ コマンド 979
show ap dot11 24ghz コマンド 1398
show ap dot11 5ghz 640, 981
show ap dot11 5ghz cleanair device type コマンド 59
show ap dot11 cleanair summary 640
show ap dot11 l2roam 636
show ap ethernet statistics 646
show ap groups 647
show ap image 648
show ap join stats summary 650
show ap link-encryption 650
show ap mac-address 651
show ap monitor-mode summary 653
show ap name 679
show ap name auto-rf 653
show ap name bhrate 656
show ap name cac voice 657
show ap name capwap retransmit 660
show ap name ccx rm 661
show ap name cdp neighbors 662
show ap name channel 662
show ap name command 655
show ap name config 663
show ap name config dot11 665
show ap name config fnf 658
show ap name config slot 668
show ap name core-dump 671
show ap name data-plane 672
show ap name dot11 673, 903
show ap name dot11 call-control 658
show ap name dot11 cleanair 676
show ap name ethernet statistics 677
show ap name eventlog 678
show ap name inventory 680
show ap name link-encryption 682

show ap name service-policy 683, 902
show ap name tcp-adjust-mss 683
show ap name wlan 684
show ap slots 686
show ap summary 687
show ap tcp-adjust-mss 688
show ap uptime 689
show auto qos コマンド 873
show avc client コマンド 1286
show avc wlan コマンド 1287
show cable-diagnostics tdr コマンド 1288
show capwap summary 181
show cisp コマンド 1121
show class-map コマンド 905
show controller utilization コマンド 194
show controllers cpu-interface コマンド 182
show controllers ethernet-controller コマンド 183
show eap コマンド 1124
show eee コマンド 195
show env xps コマンド 1297
show env コマンド 199, 1295
show errdisable detect コマンド 202
show errdisable recovery コマンド 204
show etherchannel コマンド 456
show flow exporter コマンド 120
show flow record コマンド 129
show interfaces counters コマンド 209
show interfaces switchport コマンド 212
show interfaces transceiver コマンド 214
show interfaces コマンド 205
show ip igmp snooping igmpv2-tracking コマンド 380
show ip igmp snooping wireless mcast-spi-count コマンド 384
show ip igmp snooping wireless mgid コマンド 384
show ip pim autorp コマンド 386
show ip pim bsr コマンド 387
show ip pim bsr-router コマンド 386
show ip pim tunnel コマンド 388
show ip sla statistics コマンド 783
show lacp コマンド 460
show license right-to-use コマンド 1306
show location ap-detect コマンド 1309
show location コマンド 1308
show mac address-table move update コマンド 1310
show mgmt-infra trace messages ilpower コマンド 220
show mgmt-infra trace messages ilpower-ha コマンド 221
show mgmt-infra trace messages platform-mgr-poe コマンド 222
show mod コマンド 219
show monitor session コマンド 789
show monitor コマンド 785
show network-policy profile コマンド 223
show nmsp コマンド 1311
show pagp コマンド 464
show platform capwap summary 224
show platform etherchannel コマンド 466
show platform ip multicast コマンド 393
show platform ip wccp コマンド 791
show platform pm コマンド 467
show platform software trace level 1387
show platform software trace message 1383
show platform stack-manager コマンド 1197
show platform vlan コマンド 1418
show policy-map コマンド 919
show power inline コマンド 242
show redundancy config-sync コマンド 1202
show redundancy コマンド 1198
show sampler コマンド 130
show sdm prefer コマンド 1315
show stack-power コマンド 248
show storm-control 1129
show switch コマンド 1204
show system mtu コマンド 250
show tech-support wireless コマンド 1316
show tech-support コマンド 251
show trace messages capwap ap ha コマンド 1209
show trace messages mobility ha コマンド 1210
show udld コマンド 470
show vlan access-map コマンド 1131
show vlan filter コマンド 1132
show vlan group コマンド 1133
show vlan コマンド 1419
show vtp コマンド 1422
show wireless ap summary 690
show wireless band-select コマンド 1318
show wireless client ap 690
show wireless client calls コマンド 914, 1319
show wireless client dot11 コマンド 915, 1320
show wireless client location-calibration コマンド 1321
show wireless client mac-address コマンド 916, 917
show wireless client probing コマンド 1321
show wireless client summary コマンド 1322
show wireless client timers コマンド 1323
show wireless client voice diagnostics コマンド 918, 1323
show wireless country コマンド 1324
show wireless detail コマンド 1327
show wireless dtls connections コマンド 1328
show wireless interface summary コマンド 253

show wireless ipv6 statistics コマンド 407
show wireless load-balancing コマンド 1331
show wireless media-stream group コマンド 1399
show wireless mobility 709
show wireless performance コマンド 1331
show wireless pmk-cache コマンド 1332
show wireless probe コマンド 1333
show wireless sip preferred-call-no コマンド 1334
show wireless summary コマンド 1335
show wireless vlan group コマンド 1429
show wlan コマンド 921, 1507
shutdown コマンド 1336, 1511
sip-cac コマンド 1512
snmp-server enable traps bridge コマンド 798
snmp-server enable traps bulkstat コマンド 799
snmp-server enable traps call-home コマンド 800
snmp-server enable traps cef コマンド 801
snmp-server enable traps CPU コマンド 802
snmp-server enable traps envmon コマンド 803
snmp-server enable traps errdisable コマンド 804
snmp-server enable traps flash コマンド 805
snmp-server enable traps isis コマンド 806
snmp-server enable traps license コマンド 807
snmp-server enable traps mac-notification コマンド 808
snmp-server enable traps ospf コマンド 809
snmp-server enable traps pim コマンド 811
snmp-server enable traps port-security コマンド 812
snmp-server enable traps power-ethernet コマンド 813
snmp-server enable traps snmp コマンド 814
snmp-server enable traps stackwise コマンド 815
snmp-server enable traps storm-control コマンド 818
snmp-server enable traps stpx コマンド 819
snmp-server enable traps transceiver コマンド 820
snmp-server enable traps vrfmib コマンド 821
snmp-server enable traps vstack コマンド 822
snmp-server enable traps コマンド 794
snmp-server engineID コマンド 823
snmp-server host コマンド 824
speed コマンド 254
stack-mac persistent timer コマンド 1211
stack-mac update force コマンド 1212
stack-power コマンド 256
StackPower 248, 256
standby console enable コマンド 1213
static-ip tunneling コマンド 1513
statistics airtime-fairness 985
storm-control コマンド 1134
switch priority コマンド 1216
switch provision コマンド 1217
switch renumber コマンド 1219
switch stack port コマンド 1214
switchport access vlan コマンド 475
switchport block コマンド 257
switchport mode access 830
switchport mode コマンド 477
switchport nonegotiate コマンド 480
switchport port-security aging コマンド 1137
switchport port-security mac-address コマンド 1139
switchport port-security maximum コマンド 1142
switchport port-security violation コマンド 1144
switchport priority extend コマンド 1430
switchport trunk コマンド 1431
switchport voice vlan コマンド 481
switchport コマンド 474
system env temperature threshold yellow コマンド 1336
system mtu コマンド 259

T

template data timeout コマンド 134
test ap name 691
test cable-diagnostics tdr コマンド 1338
test capwap ap name 692
test mcu read register コマンド 260
traceroute mac ip コマンド 1342
traceroute mac コマンド 1339
transport コマンド 135
trapflags ap 693
trapflags client コマンド 1345
trapflags コマンド 1344
ttl コマンド 136
type コマンド 1346

U

udld port コマンド 486
udld reset コマンド 488
udld コマンド 484
unset コマンド 1347

V

version コマンド 1349

vlan access-map コマンド 1161
vlan dot1q tag native コマンド 1441
vlan filter コマンド 1163
vlan group コマンド 1164
vlan コマンド 1434, 1514
voice vlan コマンド 263
voice-signaling vlan コマンド 262
vtp primary コマンド 1449
vtp（インターフェイス コンフィギュレーション）コマンド 1448
vtp（グローバル コンフィギュレーション）コマンド 1442

W

wgb non-cisco コマンド 1515
wireless ap-manager interface 265
wireless broadcast vlan コマンド 1450
wireless client command 401
wireless client mac-address コマンド 1352
wireless client コマンド 1349
wireless dot11-padding コマンド 1149
wireless exclusionlist command 266
wireless linktest コマンド 267
wireless load-balancing コマンド 1357
wireless management interface コマンド 268
wireless media-stream コマンド 1401
wireless mobility 701
wireless mobility controller 701, 703
wireless mobility group keepalive 705
wireless mobility group member ip 706
wireless mobility group name 707
wireless mobility load-balance 708
wireless peer-blocking forward-upstream コマンド 268
wireless security dot1x コマンド 1150
wireless security lsc コマンド 1152
wireless security strong-password コマンド 1153
wireless sip preferred-call-no コマンド 1358
wireless wps ap-authentication コマンド 1154
wireless wps auto-immune コマンド 1155
wireless wps cids-sensor コマンド 1156
wireless wps client-exclusion コマンド 1157
wireless wps mfp infrastructure コマンド 1158
wireless wps rogue コマンド 1159
wireless wps shun-list re-sync コマンド 1160
wlan shutdown コマンド 1519
wlan コマンド 1517, 1518
wmm コマンド 1520

す

スイッチド ポート アナライザ（SPAN）セッション 785, 789
スタック メンバーのプライオリティ 1216
スタック メンバ番号 1219

は

バジェット電力 166

ふ

フロー ベース SPAN（FSPAN）セッション 775
フローベース RSPAN（FRSPAN）セッション 775

り

リアルタイムの消費電力のポリシング 177
リモート SPAN（RSPAN）セッション 785, 789